OPINNÄYTETYÖ

ARI PAASONEN 2012

SANTAPARK OY:N LANGATON LÄHIVERKKO-SUUNNITELMA

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

TIETOJENKÄSITTELYN KOULUTUSOHJELMA

ROVANIEMEN AMMATTIKORKEAKOULU

LUONNONTIETEIDEN ALA

Tietojenkäsittely

Opinnäytetyö

SANTAPARK OY:N LANGATON LÄHIVERKKO-SUUNNITELMA

Ari Paasonen

2012

Toimeksiantaja Santapark Oy

Ohjaaja Martti Kemppainen

Hyväksytty _____ 2012 _____

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

Luonnontieteiden ala
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön tiivistelmä

Tekijä	Ari Paasonen	Vuosi	2012

Toimeksiantaja	Santapark Oy
Työn nimi	Santapark Oy:n langaton lähiverkkosuunnitelma
Sivu- ja liitemäärä	54

Opinnäytetyöni pohjautuu Santapark Oy:ltä saamaani toimeksiantoon, jossa tehtävänäni oli kehittää yritykselle toimiva WLAN (Wireless Local Area Network) -verkkosuunnitelma. Suunnitelman konkreettinen toteuttaminen ei ole osa tätä tutkimusta. Työn tavoitteina oli ratkaista tutkimuskysymykseni siitä, mikä on tehokkain WLAN-ratkaisu Santaparkin kaltaiselle yritykselle. Santapark Oy:n vaatimukset suunniteltavalle verkkoyhteydelle olivat toteuttaa asiakaskäyttöön suunniteltujen tilojen langattomat verkkoratkaisut sekä verkon jakamisen mahdollisuus asiakkaiden käyttöön ilman yrityksen työntekijöille tarkoitetun verkon vaarantamista.

Opinnäytetyö koostuu kahdesta osiosta: pidemmästä teoriaosuudesta sekä toimivan WLAN-ratkaisun raportista. Lähestyin aihetta kartoittamalla langattoman viestinnän tekniikkaa sekä WLAN-tekniikan kehitystä nykypäivään asti. Teoriapohjan tutustuminen vahvisti kykyjäni toteuttaa Santapark Oy:lle toimiva WLAN-ratkaisu. Opinnäytetyön tulokseksi syntyi raportti langattoman lähiverkon suunnitelmasta. Lopullinen raportti koostuu teorian avulla johdetusta tehokkaasta verkkoratkaisusta, joka täyttää yrityksen työlle asettamat vaatimukset.

Johtopäätöksenä Santapark Oy:lle tehokkain verkkoratkaisu on VLAN (Virtual Local Area Network) -tekniikka. Tämän avulla on mahdollista jakaa verkko kahteen virtuaaliseen verkkoon. Tämä on tehokkain tapa eristää asiakkaille suunniteltu verkko yritysverkosta.

Avainsanat:	WLAN, Langaton lähiverkko, Langaton viestintä, Palveluryhmät, Langattoman verkon tietoturva
Muita tietoja:	Santapark Oy yhteystiedot: www.santapark.com

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

School of Business And Administration
Business Information Technology Programme

Abstract of Thesis

Author	Ari Paasonen	Year	2012
Commissioned by	Santapark Ltd.		
Subject of thesis	Wireless Local Area Network (WLAN) plan for Santapark Ltd.		
Number of pages	54		

This thesis is based on a commission given by Santapark Ltd. The purpose of the study was to create a Wireless Local Area Network (WLAN) network plan that meets the needs of the company. The aim of the commission was to find the most efficient network solutions for a company, such as, Santapark Ltd. The commission was to design a wireless network that could be shared with customers without compromising the employee network. The actual execution of this plan is not part of this study.

The thesis is made up of two parts: the theoretical background and the report on the finished WLAN-solution. The subject was first approached by inspecting the development of the technology used in wireless communication and WLAN networks up to this day. Through familiarity with the information from the theoretical background, a working network solution for Santapark Ltd. was created.

The result of this thesis is a report on efficient network solution plan that meets the prerequisites set by the employer. It can be used as a plan which can be implemented in the future by Santapark Ltd.

Keywords: WLAN, Wireless Local Area Network, Wireless communication, Service groups, Wireless network security

More information: Santapark Ltd. contact information: www.santapark.com

SISÄLTÖ

KUVIO- JA TAULUKKOLUETTELO

1 JOHDANTO

Langattomat lähiverkot ovat yleistyneet 2000-luvun aikana räjähdysmäisesti. Alun perin aseteollisuutta varten suunnitellut langattomat viestintätekniikat ovat levinneet myös siviilimaailmaan. Kaupunkialueet ovat täynnä avoimia liityntäpisteitä, joiden avulla käyttäjä voi saada yhteyden Internetiin. Suuremmassa mittakaavassa langaton lähiverkkotekniikka on suhteellisen rajallinen, sillä päällekkäiset kanavat, häiriötä aiheuttavat laitteet sekä rajoittunut kantoalue aiheuttavat ongelmia.

Mobiliteetti ja langattomuus ovat kenties merkittävimpiä tekijöitä nykyisessä laitesuunnittelussa. Kannettavat tietokoneet, matkapuhelimet sekä erilaiset viihdelaitteet käyttävät yhä useammin jotain langatonta tiedonsiirtotapaa esimerkiksi järjestelmäpäivitysten tekoa varten. Useissa kannettavissa tietokoneissa on poistuttu normaalista verkkoliitännästä sen suuren koon takia ja siirrytty pienempiin ja markkinoilla harvemmin tarjolla oleviin kaapeliratkaisuihin. Erityisarvo tuotekehityksessä on tehokkaissa langattomissa verkkokorteissa.

Tavoitteenani on tutkia langattoman lähiverkon tekniikkaa ja teoriaa sekä laatia suunnitelma tehokkaimmasta mahdollisesta WLAN-verkkokokonaisuudesta Santapark Oy:lle. Verkkokokonaisuus tulee sisältämään sekä yrityskäytössä olevan suojatun langattoman verkon että asiakkaille suunnatun suojaamattoman verkkoalueen. Käyttämäni lähdekirjallisuus voi vaikuttaa alan tutkimuksen standardeihin verrattuna vanhentuneelta, mutta tässä tutkimuksessa sen käyttö on perusteltua. Uutta kirjallisuutta aiheesta tulee hyvin vähän, sillä langattoman verkkoon liittyvät uudistukset koskevat lähinnä standardeja, joita ilmestyy harvoin. Vanhemmankin materiaalin käyttö oli tarpeellista erityisesti tutkimuksen teoriaosuudessa. Vanhoistakin teoksista löytyvä tieto on vielä tietyissä yhteyksissä ajankohtaista.

Santapark on suosittu kohde turisteille ja vieraileville perheille. Nimensä mukaisesti yritys tarjoaa jouluaiheista toimintaa ja elämyksiä. Yrityksen tiloissa liikkuu hyvin paljon ihmisiä ja tästä syystä langattoman verkon tarjoaminen asiakkaille on järkevää. Yritys on rakennettu kallion sisään, mikä tuo muka-

naan lähiverkkosuunnitelman toteuttamiseen tapauskohtaisia erikoisvaatimuksia.

Opinnäytetyö on jaoteltu kahteen osuuteen: teoriaosuuteen sekä langattoman verkon suunnitteluun. Teoriaosuudessa käsittelen langatonta verkkotekniikkaa ja sen yleisimpiä termejä. Pyrkimyksenäni on esittää langattoman lähiverkon toiminta mahdollisimman selkeäkielisenä ja helposti lähestyttävänä. Käsittelen opinnäytetyössäni langattoman verkon toiminnan perusteita, mutta tarkoituksenani on tuoda esiin myös teknistä termistöä. Teoriaosuus on jaettu kahteen alakategoriaan: tekniikkaan sekä tietoturvaan. Tietoturva on nykyisessä yritystoiminnassa hyvin tärkeä toimintahaara, joten on aiheellista käydä asiaa tarkemminkin läpi. Pyrin rajaamaan aiheet suunnittelutyötä silmällä pitäen. Toimeksiantajan yritystiloissa on käytössä langaton verkkolaite asiakkaita varten, joka ei kuitenkaan kata riittävän suurta pinta-alaa. Tarkoituksenani on päivittää yrityksen langaton verkkotopologia riittävälle tasolle parantaen verkon toimivuutta.

Valitsin tämän aiheen opinnäytetyölleni, koska olen kiinnostunut langattomien verkkojen toimintaperiaatteista. Ohjaavan opettajan kautta sain mahdollisuuden toteuttaa oppimaani myös yritysympäristössä, joka toi käytännön lisän muuten teoriapohjaiseen työhön. Olin ollut hyvin epäileväinen langattomien verkkotekniikoiden käytännöllisyydestä isoissa tiloissa, sillä ajatus langattomasta tiedonsiirrosta vaikuttaa hyvin herkältä häiriöille sekä muille kuuluvuutta heikentäville tekijöille. Opinnäytetyöni oli minulle tilaisuus tarkistaa, olivatko ennakkoluuloni aiheellisia vai eivät.

2 LANGATTOMAT LÄHIVERKOT

2.1 Langattoman viestinnän historia ja käsitteet

Langaton viestintä on nykypäivänä hyvin yleistä, sillä matkapuhelimet, oheislaitteet sekä lähiverkot käyttävät tekniikkaa hyväkseen. Langattomalla viestinnällä on pitkä historia. Laivat ovat viestineet toisilleen valomerkkien avulla, jolloin saatiin selville laivojen sijainnit. Samoin myös Amerikan intiaanit ovat käyttäneet savumerkkejä viestintätapana, mikä mahdollisti kommunikoinnin kilometrien päähän. Vaikka nämä esimerkit eivät välttämättä vastaa nykykäsitystä langattomasta viestinnästä, niitä voidaan kutsua langattomiksi viestintätavoiksi. Langaton lähiverkko kuitenkin toimii teknisesti hyvin eri tavalla, mutta perusperiaate säilyy samana – viestintää ilman fyysistä kontaktia. (Geier 2005, 3.)

Langattoman verkkotekniikan historia alkaa 1980-luvulta. Motorolan kehittämää Altairia voidaan kutsua WLAN-tekniikan ensimmäiseksi versioksi. Tekniikka toimi kuitenkin vain Motorolan valmistamissa tuotteissa, jolloin asiakas joutui sitoutumaan käyttämään Motorolan valmistamia tuotteita. IEEE aloitti langattomien lähiverkkojen kehittämisen vuonna 1990. Työn tuloksena syntyi IEEE 802.11-standardi, mitä käytetään edelleen pohjana nykyisille ja tuleville IEEE WLAN-standardeille. (Puska 2005, 15.)

Langaton lähiverkko (WLAN) on kuitenkin tullut yleisempään käyttöön vasta viimeisen kymmenen vuoden aikana. Langattoman lähiverkon alkuvuosina tekniikkaa ei voinut suositella korvaamaan tavallista parikaapeliverkkoa. Ajan myötä tekniikka on kuitenkin kehittynyt siihen pisteeseen, että yrityksen tai kodin lähiverkko voidaan toteuttaa täysin langattomasti. Harva kuitenkaan toteuttaa kodin tai yrityksen lähiverkkoa täysin langattoman tekniikan varaan, vaan WLAN on säilyttänyt asemansa vaihtoehtoisena yhteystienä lähiverkkoon ja Internetiin.

Langaton lähiverkko käyttää radiotaajuutta tai infrapunavaloa tiedonsiirtoon. Siirretty tieto voi olla esimerkiksi sähköpostiviestejä, web-sivuja, tiedostoja, videota tai ääntä. Radioaaltoja ja infrapunavaloa käyttämällä laitteen ei tarvit-

se olla päätelaitteessa fyysisesti kiinni. Tämä helpottaa huomattavasti liikuteltavuutta, ja tämä tekee verkon käytöstä erittäin helppoa mahdollistaen työskentelyn myös työaseman ulkopuolella. (Geier 2005, 8, 54.)

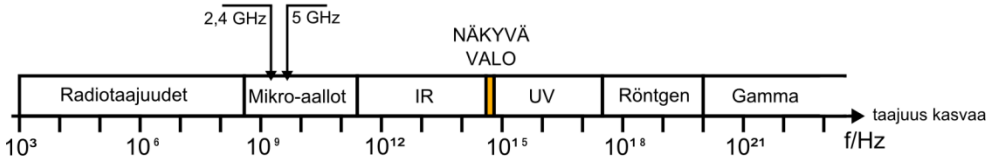
Yleinen tiedonsiirtonopeudessa ilmenevä arviointivirhe tapahtuu lähetysnopeuden määrittelemisessä. Verkkonopeuksia mitattaessa puhutaan biteistä (eng. bit tai lyhenteellä b). Yleisiä termejä ovat kilobitti (Kb tai kb), megabitti (Mb tai mb) ja gigabitti (Gb tai gb). Kilobitti on tuhat bittiä, megabitti on tuhat kilobittiä ja gigabitti on tuhat megabittiä. Yhdestä bitistä puhuttaessa tarkoitetaan joko 1 tai 0 binäärijärjestelmässä. Näitä ei saa kuitenkaan sekoittaa tiedostokokoon määriteltyyn mittayksikköön tavu (eng. Byte tai lyhenteellä B). Tavu koostuu kahdeksasta bitistä. Virheitä tämän suhteen tapahtuu hyvin usein, sillä Suomen puhekielessä bit ja byte kuulostavat lähes identtisiltä ja tästä syystä termit sekoittuvat toisiinsa. Harva lopulta kuitenkaan ymmärtää bittien ja tavujen eron. (Juuti 2009; Media Road 2011; Mitchell 2011.)

Opinnäytetyössä tiedonsiirtonopeudessa puhutaan mittayksiköllä Mbps eli toisin sanoin megabittiä sekunnissa. Todellisen tiedonsiirtonopeuden tavuiksi saadaan jakamalla bittiluku kahdeksalla. Esimerkiksi tiedonsiirron ollessa 54 Mbps on todellinen tiedonsiirto tavuina 6,75 Mt/s (megatavua/sekunnissa). (Media Road 2011.)

2.2 Signaalit langattomassa verkossa

Langattomassa lähiverkossa tieto lähetetään sähkömagneettisien signaalien eli radioaaltojen avulla (eng. Radio Frequency, RF). Kuviossa 1 voidaan nähdä langattoman verkon käyttämät radioaallot sähkömagneettisen säteilyn spektristä. Radioaallot kuuluvat analogisiin signaaleihin, sillä niiden amplitudi vaihtelee jatkuvasti ajan suhteen. Amplitudilla tarkoitetaan signaalin värähdysliikkeen laajuutta. Radioaaltojen mittayksikkönä toimii hertsi (Hz). Tietokoneet vastaavasti käyttävät digitaalisia signaaleja tiedon välittämiseen. Tietokoneen digitaaliset signaalit käsittävät binäärilukuja, joten ilmateitse lähetettävä data on ensin vahvistettava ja muutettava analogiseen muotoon. Muuntaminen tapahtuu modulaattorilla. Vastaanottaessa kohde vahvistaa

signaalin ja demoduloi signaalin modulaattorilla alkuperäiseen muotoon. (Geier 2005, 54–55, 56–57, 69.)



Kuvio 1. Sähkömagneettisen säteilyn spektri (soveltaen Puska 2005, 53)

Signaalin lähettäminen ilmateitse tapahtuu antennin avulla. Antennin tehtävänä on muuntaa sähköenergia sähkömagneettiseksi säteilyksi. Antennien lähettämä säteily on epäsymmetristä, eli signaalin lähetyskuvio voi olla esimerkiksi vaakatasossa laajempi kuin pystysuunnassa. Tähän vaikuttaa eniten käytettävä antennityyppi, kuten dipoliantenni, levyantenni, sauva-antenni, laitteen sisäiset antennit, yagi-antenni ja lautasantenni. Yleisimpinä antennityyppeinä WLAN-toteutuksissa ovat kuitenkin dipoliantennit ja laitteen sisäiset antennit. (Puska 2005, 60, 63.) Langattomasta verkkolaitteen ulkopuolella oleva taitettava antenni on lähes poikkeuksetta tyypiltään dipoliantenni (ks. kuvio 9 s.16).

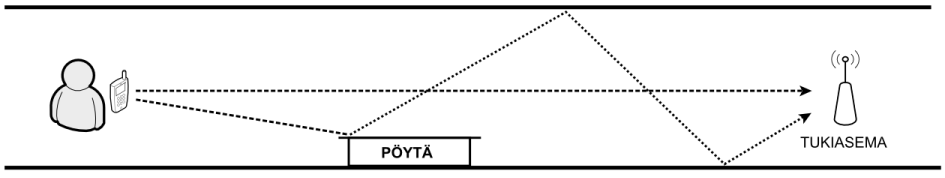
Toinen langaton tiedonsiirtotapa on infrapunavalo (Infra Red, IR). Infrapunavalon käyttäminen tiedonsiirtotekniikkana on mahdollista, kun tukiasema ja työasema ovat näköyhteydessä ja riittävän lähellä toisiaan. Signaalin kulkua heikentävät ulkopuoliset valon lähteet kuten aurinko ja yleisvalaisimet. (Granlund 2007, 70–71.) Infrapunavalon käyttö lähiverkkototeutuksissa on harvinaista johtuen lyhyestä kantamasta sekä heikosta häiriönsietokyvystä. Heikon kysynnän vuoksi yhä harvempi WLAN-tukiasema tukee IR-tekniikoita. Tästä syystä en nähnyt IR-tekniikkaa käytännöllisenä vaihtoehtona opinnäytetyöni asiakastyössä.

2.3 Signaalin eteneminen

Tyhjiössä on mahdollista saada sähkömagneettinen signaali kulkemaan suoraviivaisesti ja vaimentumatta. Todellisuudessa se kuitenkin heikkenee etäisyyden kasvaessa. Langattomien verkkojen signaalin vaimentumisen tutkimiseen käytetään vapaan tilan (yleisesti ilma) vaimentumissuhdetta (Free Space Loss), jossa laskelmallisesti selvitetään signaalin vaimeneminen vapaassa liikkuvuudessa. Tiellä ei ole mitään signaalia häiritseviä fyysisiä esteitä. (Puska 2005, 56.)

Radioaallot ovat herkkiä interferenssille, sillä laitteet eivät pysty tarkalleen erottelemaan päällekkäisiä samalla taajuudella olevia signaaleja. Interferenssi on kuitenkin yleisintä 2,4 GHz:n taajuusalueella, johtuen kapeista päällekkäisistä kanavista sekä samaa taajuutta käyttävistä muista laitteista. Häiriötekijät voidaan poistaa vaihtamalla määriteltyä kanavaa, siirtämällä verkkolaite alueelle, jossa ei ole muita häiritseviä laitteita, tai nostamalla käytettävää taajuusaluetta 5 GHz:iin. (Geier 2005, 128–129.)

Signaalin amplitudiin ja tehoon vaikuttavat heikentävästi vesi, sumu, lumi sekä rakennukset. Signaalin kuuluvuuteen vaikuttavat myös oikeassa kulmassa olevat esineet, joista signaali voi heijastua. Heijastuminen syntyy, kun signaalin tulokulma on riittävän suuri esineeseen nähden, jolloin vain osa säteilystä heijastuu pois ja osa taittuu esineen sisään aiheuttaen tiedon muuttumista (Kuvio 2). Signaali voi myös taipua, kun se joutuu vuorovaikutukseen alkeishiukkasten kanssa. Tällaisia alkeishiukkasia on ilmassa sekä erityisesti ylemmissä ilmakehän kerroksissa. (Puska 2005, 57–58.)

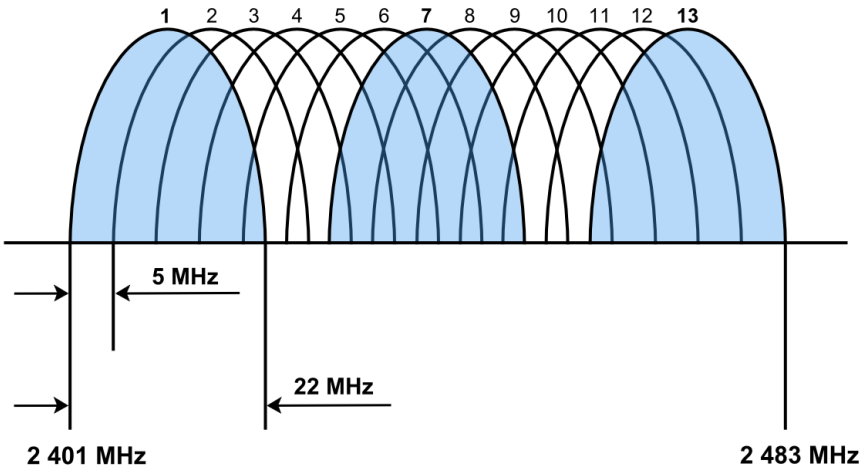


Kuvio 2. Signaalin heijastuminen (soveltaen Geier 2005, 74)

2.4 Taajuusalueet ja kanavat

Langattomilla lähiverkoilla on käytössään ennalta määritellyt taajuusalueet 2,4 GHz ja 5 GHz sekä sovitut kaistan leveydet. Kaista on jaettu myös ennalta määriteltyihin kanaviin, joita laitteet käyttävät viestintään. Bluetooth-laitteet sekä mikroaaltouunit käyttävät 2,4 GHz:n taajuusaluetta, mikä voi ajoittain aiheuttaa interferenssiä langattomassa lähiverkossa heikentäen suorituskykyä.

Langattomissa lähiverkoissa on yleisempänä taajuusalueena käytössä 2,4 GHz. Kaistan leveys ja taajuusalue riippuu maantieteellisestä sijainnista. Euroopassa kaistan leveys on 85 MHz ja se toimii välillä 2,400–2,485 GHz. Taajuusalue on jaettu Euroopassa 13 kanavaan jokainen leveydeltään 22 MHz. Yhdysvalloissa kanavia on käytössä 11. Jokainen kanava on 5 MHz:n välein, joten kanavat ovat osittain limittäisiä. Kuviossa 3 voidaan nähdä 802.11-standardin taajuusalueen kanavat sekä sinisellä värillä korostetut kolme toisiaan häiritsemätöntä kanavaa. Euroopassa toisiaan häiritsemättömät kanavat ovat 1, 7 ja 13 (vaihtoehtoisia kanavia ovat 1, 6, 13 ja 1, 8, 13) ja Yhdysvalloissa kanavat 1, 6, 11. (Puska 2005, 39.)



Kuvio 3. IEEE 802.11 2,4 GHz:n taajuusalueen kanavat (Puska 2005, 39)

Korkeammalla 5 GHz:n taajuusaluella on käytettävissä 12 toisiaan häiritsemätöntä kanavaa, joista jokaisen kaistan leveys on 20 MHz. Tämän ansioista yhteys on vakaampi ja luotettavampi. Käyttäessä 5 GHz:ä pystytään toteut-

tamaan lähestulkoon häiriötön WLAN-verkko. Bluetooth-laitteet tai mikroaaltouunit eivät häiritse signaalia. Korkeampi taajuusalue kuitenkin heikentää signaalin kantavuusaluetta sekä läpäisykykyä. Korkeampaa taajuutta käyttävien laitteiden suosio ei ole yleistynyt laitteiden korkeamman hinnan sekä yhteensopivuusongelmien takia. (Geier 2005, 128–129.) Santapark Oy:n toteutuksessa en tule käyttämään 5 GHz:n taajuusaluetta.

Nykyaikaisissa tukiasemissa on käytössä auto-channel -toiminto, jonka avulla tukiaseman taajuuskanavan valinta tapahtuu automaattisesti. Tukiasema selvittää ympärillä olevien radiosignaalien taajuudet sekä niiden käyttämät kanavat. Tukiasema valitsee vähiten toisia kanavia häiritsevän vaihtoehdon. Tämä ei kuitenkaan ole aina hyvä vaihtoehto. Omakohtaisten kokemusten perusteella olen huomannut, että useamman tukiaseman käyttäessä auto-channel -toimintoa on kanavien vaihtelu hyvin summittaista ja signaalin vahvuus vaihtelee huomattavasti. Parhaaksi vaihtoehdoksi olen havainnut kanavan valitsemisen manuaalisesti 1, 7 ja 13 välillä.

2.5 OSI-malli

Suuret tietokonevalmistajat IBM (International Business Machines) ja DEC (Digital Equipment Corporation) aloittivat verkkotekniikoiden kehittämisen 1960-luvun lopulla. IBM kehitti oman verkkomallinsa SNA-verkon (Systems Network Architecture) ja DEC oman DECnetin. Ongelmiksi kuitenkin ilmenivät verkkojen rakenteelliset eroavaisuudet sekä yhteensopivuusongelmat. Versioiden välille kehitettiin yhteensopivuuden mahdollistavia yhdyskäytäviä, mutta ratkaisu ei ollut pitkäaikainen. (Odom 2005, 47–49.)

Täydellisen yhteensopivuuden varmistamiseksi kaikki suurimmat tietotekniikkayritykset (mm. IBM, DEC, Apple ja Microsoft) luopuivat valmistajakohtaisista standardeistaan ja siirtyivät käyttämään avointa verkkomallia. Nykypäivänä lähes kaikki verkkolaitteet käyttävät samaa standardia nimeltään TCP/IP (Transmission Control Protocol/Internet Protocol). (Odom 2005, 49.)

Lähiverkon arkkitehtuurin kattavin ja monipuolisin kuvausmalli on ISO:n (International Standards Organization) kehittämä seitsemänkerroksinen OSI-

malli (Open Systems Interconnect). OSI-malli ryhmittelee lähiverkon toiminnot omiin kerroksiin, jolloin langattoman verkon toimintaa on helppo tarkastella. Jokainen OSI-mallin kerros tukee yläpuolellaan olevaa kerrosta. (Geier 2005, 52–54.)

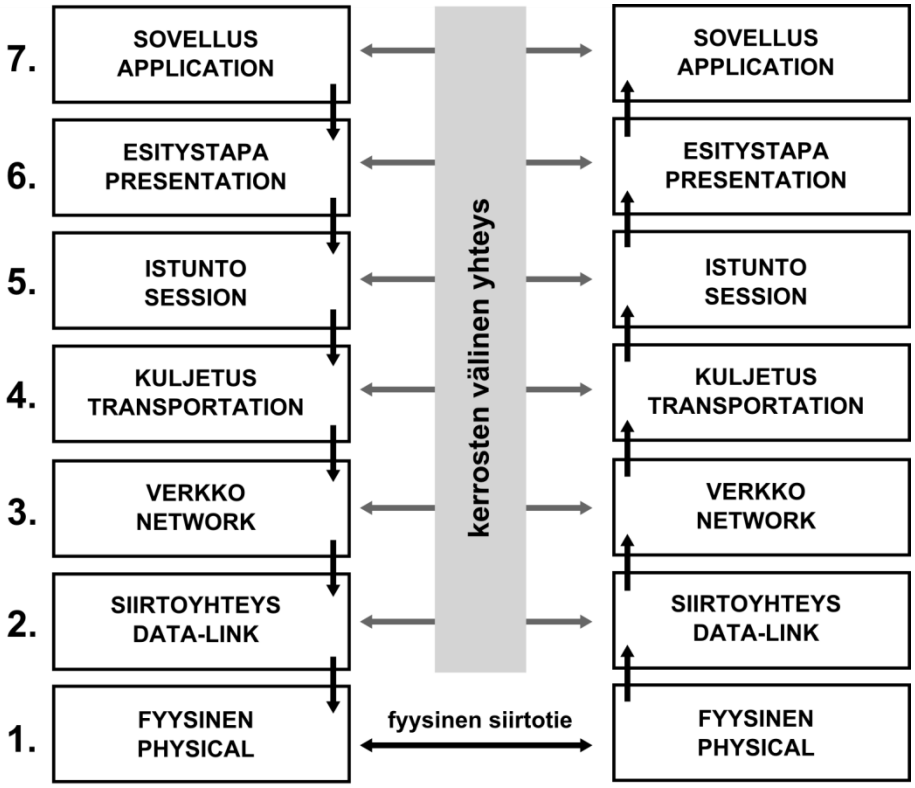
OSI-mallin ensimmäinen kerros on nimetty **Fyysiseksi kerrokseksi** (eng. Physical Layer). Kerros määrittelee laitteistojen fyysisen kaapeloinnin sekä signaalin siirtämiseen liittyvät tiedot. Fyysiseen kerrokseen kuuluvat muun muassa signaalien jännitetasot, kaapelityypit, vaimennus, ylikuuluminen ja liitintyypit. (Hakala – Vainio 2005, 139.) Ethernet, Wi-Fi, Bluetooth ovat esimerkkejä ensimmäisen kerroksen standardeista ja protokollista (Rackley 2007, 10).

OSI-mallin toinen kerros on **Siirtotieyhteys** (Data Link Layer). Se käsittelee tietoverkon datan lähettämiseen liittyviä tekniikoita, kuten kehysten muodostamisesta ja lähettämisestä. Kerros myös selvittää vastaanottavan ja lähettävän osapuolen MAC-osoitteet. Verkkokortit, sillat sekä kytkimet ovat kerroksen keskeisimpiä aktiivilaitteita. (Hakala – Vainio 2005, 139.) 802.11-standardit kuuluvat siirtotieyhteys-kerrokseen (Rackley 2007, 10).

Muita OSI-mallin kerroksia ovat **Verkkokerros (Network Layer)**, joka määrittelee tietoliikenteen väliset reititykset sekä verkkoliikenteen priorisointimääritykset. IP-protokollat kuuluvat verkkokerrokseen. **Kuljetuskerros (Transport Layer)** on ensimmäinen ohjelmallinen kerros. Kuljetuskerros huolehtii kuljetusprotokollasta, kuten TCP-protokollasta. Seuraava OSI-mallin kerroksista on **Istuntokerros (Session Layer)**, jonka tehtäviin kuuluvat käyttöoikeuksien tarkistukset sekä muut suojaukseen liittyvät tehtävät. Kuudes kerros käsittää **Esitystapakerroksen (Presentation Layer)**, joka määrittelee palvelimen ja käyttäjän välisen liikenteen muodon. Tiedonsiirto järjestelmien välillä tapahtuu binäärilukuina, joten esityskerros huolehtii tiedon moduloinnista ja demoduloinnista. OSI-mallin ylin kerros on nimeltään **Sovelluskerros (Application Layer)**, jonka tarkoituksena on määritellä sovellusten ja käyttöjärjestelmien osat, joita ei alemmissa kerroksissa ole määriteltyinä. Nykyisissä lähiverkoissa ei ole mahdollista erotella sovellus-, esitystapa- ja istuntokerroksia

itsenäisiin osiin, vaan kerrokset muodostavat yhden suuren ohjelmallisen kokonaisuuden. (Hakala – Vainio 2005, 139–141.)

OSI-mallin toiminta tapahtuu ylimmästä kerroksesta alaspäin (Kuvio 4). Tieto siirretään kerroksesta toiseen palvelupyynnöllä. Palvelupyyntö otetaan vastaan aina OSI-mallin ylemmältä kerrokselta. Tulevilla palvelupyynnöillä ei tieto siirry suoraan kerroksissa ylöspäin, vaan jokainen kerros käsittelee datakehyksen ylemmälle kerrokselle sopivaan muotoon. Loogisella tasolla tieto siirretään suoraan kerrokselta toiselle, mutta fyysinen tiedonsiirto voi tapahtua vain fyysisen kerroksen kautta. (Granlund 2007, 10; Rackley 2007, 10.)



Kuvio 4. OSI-mallin tiedonkulku kerrosten välillä (Hakala – Vainio 2005, 138)

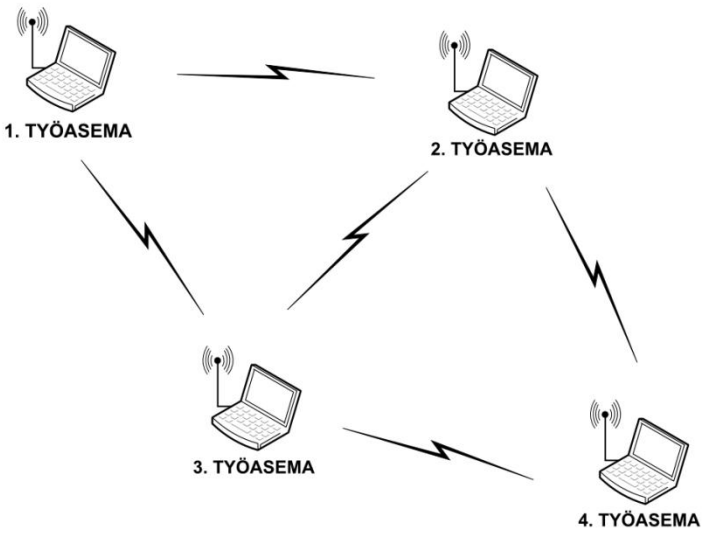
2.6 WLAN-verkkojen topologiat

Lähiverkko voidaan rakentaa usealla eri rakenneratkaisulla eli topologialla. Aivan kuten parikaapeliverkossa, myös langattomissa lähiverkoissa topologiaan vaikuttavat verkkolaitteet sekä perusvaatimukset verkolle. Langattomien verkkojen topologiat kuitenkin jakautuvat kolmeen pääryhmään: IBSS, BSS ja ESS.

2.6.1 Independent Basic Service Set

Itsenäinen palveluryhmä eli Independent Basic Service Set (IBSS) on langattoman verkon topologioista yksinkertaisin ratkaisu. Ajoittain IBSS-verkkoa kutsutaan myös nimellä Ad-Hoc -verkko. Viestintä tapahtuu laitteiden välillä ilman pääteasemaa ja yhteyttä kiinteään verkkoon. Kuviossa 5 on esitetty Ad-Hoc -verkon yksinkertainen malli. Kyseistä verkkotopologiaa ei kuitenkaan suositella muille kuin pienille työryhmille ja tilapäiseen lähiverkon tarpeeseen. Tällaisia tilanteita ovat muun muassa kokous- tai neuvottelutilanteet. Tiedonsiirtonopeus sekä toimivuus IBSS-verkossa eivät ole yhtä edistyksellistä kuin BSS- tai ESS verkkotopologiassa. (Granlund 2007, 294–295.)

IBSS-verkko on myös herkkä rakenteenmuutoksille laitetta siirrettäessä kuuluvuusalueen rajalle. Niin sanotulla piiloasemalla (hidden station) tarkoitetaan tilannetta, kun kaksi samassa verkossa olevaa laitetta eivät kuule toisiaan. Tämä estää tiedonsiirron sekä kommunikoinnin asemien välillä. Kuvio 5:n työasema 1. ja työasema 4. eivät pysty kommunikoimaan keskenään, sillä niiden välinen etäisyys on liian suuri. IBSS-verkon suositukset eivät mahdollista jonkin aseman toimivan reitittimenä siirtäen datakehyksiä piiloasemille. (Granlund 2001, 231.) Käytännöllisistä syistä IBSS-verkkotopologiaa ei tulla käyttämään Santapark Oy:n lähiverkkosuunnitelmassa.

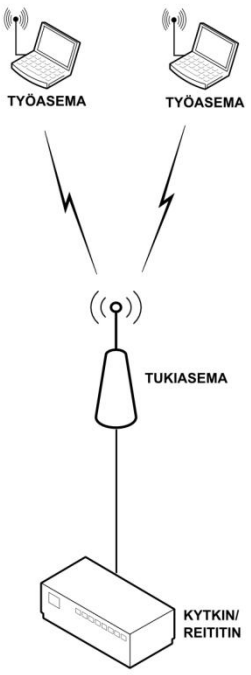


Kuvio 5. IBSS-verkkotopologia ja hidden station -ongelma (soveltaen Microsoft 2012)

2.6.2 Basic Service Set

Peruspalveluryhmä eli Basic Service Set (BSS) on yleisimmin käytössä oleva langattoman lähiverkon topologia koti- ja pienyritysverkoissa. Toisin kuin IBSS-verkossa, BSS-topologiassa kaikki verkon laitteet ovat yhteydessä pääteasemaan (usein kytkin, reititin tai tukiasema), joka taas on kytkettynä Ethernet-verkkoon. Kaikki liikenne langattomassa verkossa tapahtuu tukiaseman kautta (Kuvio 6). BSS-topologia muistuttaakin rakenteeltaan hyvin paljon Ethernet-lähiverkkoa. (Granlund 2007, 295.)

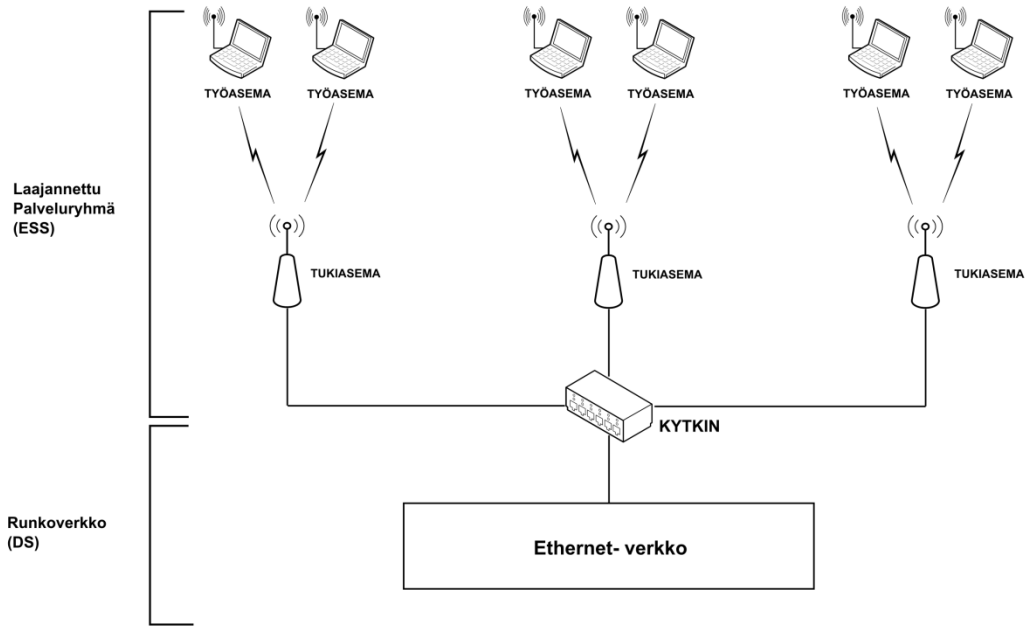
BSS-verkko on kuitenkin riippuvainen tukiasemasta, sillä ilman tukiasemaa liikenne lakkaa työasemien välillä. Tukiaseman rikkoutuminen tai sammuminen myös sulkee mahdollisuuden verkkoviestintään lähiverkon ulkopuolelle. BSS-topologia myös rasittaa verkkoa enemmän kuin IBSS-verkko, sillä datakehys on ensin lähetettävä tukiasemalle ja sitä kautta halutulle työasemalle jolloin lähiverkon sisäinen liikenne kaksinkertaistuu. (Granlund 2001, 232.) BSS-verkkotopologia on yleisin kotien ja pienyritysten langattomissa verkkoratkaisuissa, joissa käytössä on yksi WLAN-liityntäpiste.



Kuvio 6. BSS-verkkotopologia (soveltaen Microsoft 2012)

2.6.3 Extended Service Set

Laajennettu palveluryhmä eli Extended Service Set (ESS) on mahdollista toteuttaa asentamalla useita tukiasemia samaan runkoverkkoon (Backbone network). ESS-verkkotopologian avulla on mahdollista toteuttaa koko rakennuksen kattava langaton lähiverkko (Kuvio 7). Tästä syystä se on yleisimmin käytössä oleva verkkotopologia. Laajennettu palveluryhmä antaa myös mahdollisuuden verkossa vapaaseen liikkuvuuteen tukiasemien välillä. Tätä tekniikkaa kutsutaan myös Roaming-tekniikaksi. (Granlund 2007, 296.)



Kuvio 7. ESS-verkkotopologia ja runkoverkko (soveltaen Microsoft 2012)

Roaming mahdollistaa tukiasemilta toiselle liikkumisen ilman huomattavissa olevaa viivettä tai datahävikkiä. Ongelmia voi kuitenkin ilmetä, jos laitetta liikutetaan paikasta toiseen huomattavalla nopeudella, jolloin datan häviäminen on mahdollista. Laite ei mahdollisesti ehdi vaihtaa käyttämäänsä tukiasemaa käyttäjän huomaamatta. Luvusta 2.8.5 Roaming löytyy tarkemmat määritelmät tekniikasta.

ESS-verkkotopologian taustalla oleva runkoverkko (Distribution System, DS) mahdollistaa muun muassa oikeutetun työaseman liittymisen verkkoon autentikointipalvelun avulla sekä verkosta poistumisen autentikoinnin lopetus-

palvelulla. Siirtotien suojauspalvelu mahdollistaa liikenteen seurannan autentikoituneille työasemille. Tiedonsiirtopalvelu mahdollistaa tietojen siirtämisen kahden työaseman välillä. Sidonta ja uudelleensidonta mahdollistavat tietylle asemalle tarkoitetun liikenteen ohjaamisen tukiasemalle ja työaseman siirtyessä tukiasemalta toiselle. Sidonnan purku tapahtuu irtautuessa sidotusta tukiasemasta. Reitityspalvelu mahdollistaa tukiasemien vastaanottavan osapuolen sijainnin selvittämisen. Integrointipalvelu huolehtii 802.11-verkon ja muiden verkkojen välisestä rajapinnasta. (Granlund 2001, 232–233.)

Santaparkin toteutuksessa tullaan käyttämään ESS-topologiaa, sillä tukiasemia on useita. Roaming-verkkovierailutekniikka on otettava myös mahdollisuudeksi tulevaisuudessa.

2.7 Langattoman lähiverkon laitteet

2.7.1 WLAN-kortit

Jokainen langatonta verkkoa käyttävä laite tarvitsee oikeanlaisen verkkokortin (Network interface Card, NIC) toimiakseen. Ilman korttia laite ei voi tunnistaa alueella olevia langattomia verkkoja eikä kommunikointi ilmateitse ole mahdollista. Korttien ulkonäkö ja liitäntävaihtoehdot (PCI, USB, PC) vaihtelevat laitevalmistajien kesken. (Rackley 2007, 45–46.) Kuviossa 8 on esimerkki PCI-väylään liitettävästä langattomasta verkkokortista.

Kuvio 8. PCI-väylään liitettävä langaton verkkokortti

WLAN-kortissa on usein irrotettava, ulkoinen antenni, jonka voi tarvittaessa korvata eritehoisella antennilla. Valmistajien väliset erot verkkokorteissa ovat pieniä, sillä maksimaalisen lähetystehon on oltava säädösten mukainen. Verkkokortin käyttämä standardi taas takaa yhteensopivuuden muiden laitteiden kanssa. Nykyään lähes kaikissa myydyissä kannettavissa tietokoneissa ja uusissa älypuhelimissa on sisäänrakennettu verkkokortti. (Rackley 2007, 45–46.)

2.7.2 WLAN-tukiasema

Langaton tukiasema (Access Point, AP) on yleinen osa verkkotopologiaa. Tukiaseman tarkoituksena on jakaa langallinen Ethernet-verkko ilmateitse. Tästä syystä tukiasema onkin yleisesti kytkettynä fyysisesti parikaapeliverkkoon. Tukiasemalla voi olla myös muita vaihtoehtoisia toimintoja. (Rackley 2007, 46.) Se voi toimia muun muassa **yhdyskäytävänä**, jolloin käytettävänä palveluina on muun muassa reititys, NAT, DHCP ja VPN. Jotkin tukiasemat voivat toimia myös **kytkin HUB**:ina, jos tukiaseman takana on vaihtoehtoisia RJ-45-kytkentäpaikkoja. Näihin vapaisiin portteihin voidaan liittää muita verkkolaitteita parikaapelin avulla. Jotkin tukiasemat mahdollistavat sen toimimisen **toistimena** tai **langattomana siltana**. Toistin mahdollistaa nimensä mukaisesti verkon toistamisen tukiasemien välillä laajentaen kuuluvuusaluetta. Langaton silloitus mahdollistaa kahden verkon yhdistämisen toisiinsa langattomasti. Markkinoiden uusissa tukiasemissa on myös **tiedostopalvelumahdollisuus**, kun laitteeseen liitetään esimerkiksi ulkoinen kiintolevy. (Rackley 2007, 47.)

Näitä lisäominaisuuksilla varustettuja tukiasemia kutsutaan nimellä ”lihava” AP (eng. ”fat” AP). Vaihtoehtoisesti on tarjolla myös tukiasemamalleja, joista vaihtoehtoiset ominaisuudet on karsittu pois ja konfiguroinnin on tarkoitus tapahtua runkoverkon kytkimen kautta. Näitä karsittuja versioita (Kuvio 9) kutsutaan nimellä ”laiha” AP (eng. ”thin” AP). (Rackley 2007, 47.)

Kuvio 9. Langaton Linksys-tukiasema kahdella dipoliantennilla

2.7.3 WLAN-kytkin

Suurissa yrityksen verkkokokonaisuuksissa voi olla käytössä kymmeniä, ellei satoja WLAN-tukiasemia. Näiden kaikkien tukiasemien yksittäinen asentaminen ja konfigurointi voi olla haasteellista ja erittäin aikaa vievää. WLAN-kytkimen (WLAN Switch, WLAN Controller tai Access Router) tarkoituksena on yksinkertaistaa laitteiden asentamista ja hallintaa. Se tarjoaa keskitetyn hallinnan konfigurointiin, turvallisuuteen, laadunvalvontaan sekä ongelmien ratkaisuun. (Rackley 2007, 48.)

WLAN-kytkin on sekä taloudellisesti, hallinnallisesti, toiminnallisesti että päivityksellisesti erittäin käytännöllinen ratkaisu. Kytkimeen liitettyjen tukiasemien ei tarvitse olla hinnallisesti kalliimpia ”lihavia” malleja, vaan edullisemmat ”laihat” mallit käyvät erinomaisesti. Verkkoa on helppo hallinnoida ja asetusten säätäminen tapahtuu yhdestä paikasta. Keskitetty hallintajärjestelmä säästää huomattavan määrän aikaa ja rahaa. Verkkovierailu on optimaalinen WLAN-kytkinratkaisuissa, sillä tukiasemien vaihdossa tapahtuvat toimenpiteet ovat huomattavasti nopeampia. Verkon laajentaminen ja päivittäminen on helppoa, sillä päivittäminen tapahtuu kytkimen tasolla eikä tukiasematasolla. Tar-

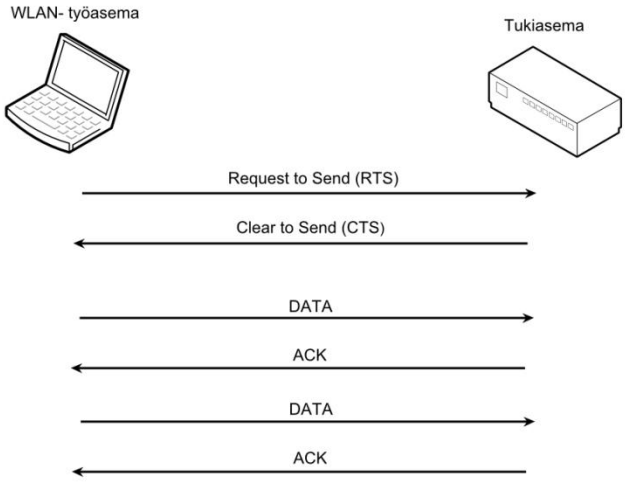
vetta WLAN-kytkimeen ei ole, jos yrityksen tiloissa ei ole huomattavaa määrää tukiasemia. (Rackley 2007, 48.)

2.8 Langaton lähiverkkotekniikka

2.8.1 Vuoronvaraus ja törmäyksen välttäminen (CSMA/CA)

Vuoronvaraus ja törmäyksen välttäminen (Carrier Sense Multiple Access/Collision Avoidance) on tärkeä tekniikka langattoman lähiverkon tiedonsiirrossa. Vuoronvarauksen tarkoituksena on estää päällekkäiset kehysten lähetykset ja niistä syntyvät kehysten törmäykset. Liikenteen kuuntelua ja hallintaa varten on tarjolla kaksi vaihtoehtoa langattoman lähiverkon liikenteen järjestelemiseen. WLAN:in käyttämä CSMA/CA muistuttaa hyvin paljon Ethernet-verkossa käytettävää CSMA/CD-tekniikkaa (Carrier Sense Multiple Access/Collision Detection). (Puska 2005, 29.)

CSMA/CA sisältää VCS-tekniikan (Virtual Carrier Sense) eli virtuaalisen kantoaallon kuuntelun. Yhteyspiste voi tällä tekniikalla hallita verkkoa käyttävien laitteiden tietoliikennettä. VCS-tekniikan toimintaperiaate on yksinkertainen. Työasema pyytää ensin yhteyspisteeltä luvan RTS-sanomalla (Request to Send) ennen datakehyksien lähettämistä. Yhteyspiste vastaa kyselyyn CTS-sanomalla (Clear to Send), jos verkko on vapaa. Tämän jälkeen työasema voi lähettää datakehyksensä. Jokainen datakehys kuitataan erikseen ACK-sanomalla (Kuvio 10). (Puska 2005, 29.)



Kuvio 10. Työaseman ja tukiaseman välinen RTS/CTS-viestitys (soveltaen Puska 2005, 29)

CSMA/CA sisältää myös PCS-tekniikan (Physical Carrier Sense), minkä vuoksi ennen datakehyksen lähettämistä aseman on selvitettävä verkon käyttämättömyys. Jos laite kuunnellessa havaitsee siirtotien olevan varattu, eli jos toinen laite on lähettämässä datakehyksiä, odottaa kuunteleva laite satunnaisen ajan, jonka jälkeen yrittää datakehyksen lähettämistä uudelleen. (Puska 2005, 30.)

Joissain tapauksissa on kuitenkin mahdollista, että datakehykset törmäävät toisiinsa. Törmäys tapahtuu, kun kaksi laitetta pyrkii lähettämään omia datakehyksiään samanaikaisesti. Tämän aiheuttaa signaalin etenemisviive, sillä signaalin eteneminen ei ole välitöntä. (Geier 2005, 60.) Datakehysten törmäykseen voi aiheuttaa myös IBSS-verkkotopologiassa ilmenevä piiloaseman ongelma eli niin sanottu hidden station -ongelma (ks. kuvio 5 s.16).

2.8.2 Monikantoaaltomodulointi (OFDM)

Monikantoaaltomodulointi (Orthogonal Frequency Division Modulation) perustuu datan siirtämiseen useilla taajuuksien alikanavilla. Datan siirtoon tarkoitettu taajuusalue jaetaan pienempiin alikanaviin. Lähettäjä ja vastaanottaja tutkivat siirtotien käyttömahdollisuuksia. Jonkin valituista taajuusalueista ollessa varattuna, valitsevat osapuolet signaali–kohinasuhteen perusteella jokaiselle alikanavan kantoaallolle sopivan modulointimenetelmän. OFDM-moduloinnin hyötynä on mahdollisuus venyttää yksittäisen bitin kestoa, jolloin saadaan huomattavasti parempi häiriösietokyky. (Granlund 2007, 112–113.)

2.8.3 Taajuushyppelyhajaspektri (FHSS)

Taajuushyppelyä (Frequency Hopping Spread Spectrum) eli FHSS-tekniikkaa on ollut käytössä jo aikaisessa sotilasteknologiassa. Taajuushyppelyssä nimensä mukaisesti päätelaitteet ”hyppivät” eri kanavien välillä lähettäen datapaketteja. FHSS-tekniikan periaatteeseen kuuluu kolme vaihetta: Datakehyksen siirtoaika jaetaan kiinteisiin aikaväleihin, käytössä olevan siir-

tokaista jaetaan alikanaviin sekä hyppelyjärjestyksen asettaminen lähettäjän ja vastaanottajan välillä. (Granlund 2007, 116–117.)

Taajuushyppely jaetaan kahteen eri luokkaan taajuushyppelyn nopeuden perusteella. SFH eli Slow Frequency Hopping on hidasta taajuushyppelyä joka syntyy, kun taajuutta vaihdetaan hitaammin verrattuna symbolin kestoon. Vastakohtana hitaalle hyppelylle on FFH eli Fast Frequency Hopping. (Granlund 2007, 117.)

Suositeltavaa on, että taajuushyppely käyttää joka seitsemättä kanavaa lähettämiseen. Tällä tavoin saadaan riittävä hyöty taajuushyppelytekniikasta. Taajuushyppelyssä on huomattavia hyötyjä tietoturvaan ja häiriösietokykyyn. Salakuuntelu on lähes mahdotonta, sillä hyppely on niin nopeaa, ettei liikenteen seuraaminen ole mahdollista, vaikka salakuuntelija tietäisikin taajuushyppelyn järjestyksen. Datakehysten törmäykset ja siitä aiheutuvat datan hävikit ovat harvinaisia, sillä lähetystiheys on hyvin nopeaa. Olisi hyvin epätodennäköistä, että kaksi datakehystä lähetetään samalla taajuushyppelykanavalla samaan aikaan. (Granlund 2007, 116.)

2.8.4 Suorasekvenssihajaspektri (DSSS)

Suorasekvenssihajaspektri (Direct Sequence Spread Spectrum) on IEEE:n 802.11b-standardissa käyttämä hajaspektritekniikka. Siinä signaali levitetään laajemmalle taajuuskaistalle. Tämä tapahtuu lähtevän signaalin kertomisella hajautusavaimen kanssa. Hajautusavain koostuu lastuista (toiselta nimeltään mikrobitti, eng. Chip). 802.11b-standardissa hajautusavain on pituudeltaan 11-lastua. Lähetettävän datankehyksen taajuuden ollessa pienempi kuin hajautusavain syntyy tästä hajautusavaimen mukainen kehys kertolaskun avulla. Loogisesti vastaanotettu hajautusavaimen mukainen kehys kerrotaan hajautusavaimen taajuudella, jolloin palataan takaisin kapeakaistaiseen alkuperäiseen signaaliin. (Granlund 2007, 117–118.)

Suorasekvenssihajaspektrin hyötynä on sen korkea häiriönsietokyky. Sietokyky on kuitenkin kytkettynä lastunopeuden ja datanopeuden suhteeseen. Mitä suurempi suhde on (lastua/s suhteessa bittiä/s), sitä parempi on verkon

häiriösietokyky. Tästä johtuen esimerkiksi 20 MHz:n kaistanleveydellä toimivaan järjestelmään on vaikea saada korkeaa tiedonsiirtonopeutta. (Granlund 2007, 118.)

2.8.5 Roaming

Vaikka Roaming ei tarkalleen ottaen kuulu yllä mainittujen WLAN-tekniikoiden ryhmään, on sitä kuitenkin tärkeää käsitellä langattoman lähiverkkotekniikan osiossa. Roaming tai suomeksi verkkovierailu on usein tutumpi termi matkapuhelinverkoista, kun matkapuhelin vaihtaa tukiasemasta toiseen ilmoittamatta siitä käyttäjälle. Tämä on yleinen toimenpide, joka mahdollistaa laitteen yhä vapaamman liikuteltavuuden. Roaming on mahdollista myös langattomissa lähiverkoissa, jolloin verkkoa käyttävä laite valitsee käytettävän tukiaseman kuuluvuuden, ruuhkaisuuden tai etäisyyden perusteella (McKeag 2004). Siirto tapahtuu käyttäjän huomaamatta, mikä lisää käyttömukavuutta.

Verkkovierailu on mahdollista toteuttaa kahdella eri tavalla. Roaming voi tapahtua kahden sellaisen tukiaseman välillä, jotka toimivat samassa aliverkossa. Saman aliverkon väliset tukiaseman vaihdokset tapahtuvat ilman häiriöitä, sillä siirtyvän laitteen ei tarvitse vaihtaa IP-osoitettaan. Tätä kutsutaan tason 2 verkkovierailuksi. Toinen verkkovierailumenetelmä mahdollistaa kahden eri verkon välisen vierailun, jolloin tukiasemavaihdoksen yhteydessä siirtyvä laite vaihtaa IP-osoitteensa uuden tukiaseman verkon mukaan. Tätä kutsutaan tason 3 verkkovierailuksi. (Home WLAN.)

Jotta verkkovierailu toimii parhaalla mahdollisella tavalla, on varmistettava tukiaseman asetusten identtisyys. Kaikkien verkkovierailua käyttävien tukiasemien täytyy jakaa sama SSID-tunnus. Salaustekniikoiden tulee olla identtisesti asetettuja, jolloin ristiriitaisia avaimia ei ilmene. Tukiasemiin on myös parasta asettaa kanavat toisiaan häiritsemättömäksi. Kanavat 1, 6 ja 13 ovat toisiaan häiritsemätöntä. Jos tukiasemia tulee olemaan yli kolme, on huomioitava, että saman taajuuskanavan jakavat laitteet ovat riittävällä etäisyydellä toisistaan. (Home WLAN.)

SSID tulee englannin sanoista Service Set Identifier eli palveluryhmätunnus (langattomien lähiverkkojen tunnus). Langattomien lähiverkkojen tunnuksen avulla samalla alueella toimivat langattoman lähiverkot voidaan erotella toisistaan. SSID-tunnus lisätään jokaiseen lähetettyyn datakehykseen, jolloin vastaanottava tukiasema voi tunnistaa sille tarkoitetut kehykset. SSID-tunnuksen lähetys voidaan kytkeä myös pois päältä, jolloin tukiaseman alueella olevat laitteet eivät löydä kyseistä verkkoa. Käyttäjän on asetettava SSID-tunnus manuaalisesti liittyäkseen kyseiseen verkkoon. Tämän tarkoituksena oli lisätä tietoturvaa ja rajoittaa verkon näkyvyyttä, mutta todellisuudessa piilossa pysyvän SSID-tunnuksen voi saada selville Internetistä löytyvien apuohjelmien avulla.

2.9 WLAN-STANDARDIT

2.9.1 IEEE 802.11

Langattomien lähiverkkojen standardeja on markkinoilla useita, mutta lähes kaikki standardit ovat lähtöisin IEEE:n (Institute of Electrical and Electronics Engineers) 802.11-standardista. IEEE:n LMSG (LAN/MAN Standarization Group) aloitti 1990-luvun alussa langattomien lähiverkkojen kehittämistyön. Kehittämistyön tuloksena IEEE ratifioi 802.11-standardin vuonna 1997. Langattomat verkot yleistyivät kuitenkin vasta vuonna 2001 hintojen putoamisen seurauksena. IEEE jatkaa edelleen 802.11-standardin kehittämistä. (Geier 2005, 118; Puska 2005, 15.)

Standardi kattaa 2,4 GHz:n taajuusalueen ja käyttää hyväkseen FHSS- ja DSSS-tekniikkaa. 802.11-standardin maksiminopeus on 2 Mbps. Taajuushyppelykuviot mahdollistavat 15 tukiaseman toimimisen samalla alueella. Hitaan maksiminopeutensa takia standardia ei suositella käytettävän sisätilaratkaisuissa, mutta standardi tarjoaa erittäin hyvän ratkaisun ulkotiloissa toimiviin järjestelmiin. DSSS-tekniikka on yhteensopiva 802.11b-standardin kanssa, mutta 802.11 DSSS-verkkokortteja ei ole enää saatavilla. Standardi sisältää myös infrapunavaloa käyttävän fyysisen kerroksen, mutta tekniikkaa käyttäviä laitteita ei ole. (Geier 2005, 118, 124.)

2.9.2 Yleiset 802.11-standardit

IEEE toi markkinoille **802.11a-standardin** vuonna 1999, mutta kyseistä tekniikkaa tukevia laitteita oli tarjolla vasta 2000-luvun alussa johtuen 5 GHz:n alueella toimivien piirien kehittämisongelmista (Geier 2005, 124). Standardi toimii 5 GHz:n taajuusalueella (5,150–5,825 GHz) käyttäen OFDM-tekniikkaa 54 Mbps:in enimmäisnopeudella. Standardissa on käytössä kolme 100 MHz:n taajuuskaistaa, joista jokaiseen on sovittu maksimilähetysteho (5,15–5,25 GHz 40mW, 5,25–5,35 GHz 200mW ja 5,725–5,825 GHz 800mW). Jokainen taajuuskaista on jaettuna neljään vapaasti käytettävään kanavaan. (Puska 2005, 45.) 802.11a:n tarjoama 54 Mbps:in enimmäisnopeus on usein vain suuntaa antava teoreettinen lähetysnopeus. Todellisuudessa lähetysnopeus vastaa noin 32 Mbps. (Jaakohuhta 2005, 268.)

802.11a:n tekniikassa on sekä hyvät että huonot puolensa. 5 GHz:n taajuusalue toi mahdollisuuden nopeampaan tiedonsiirtoon verrattuna 2,4 GHz:n WLAN-verkkoihin. Se on myös suojassa interferenssiltä, jota esimerkiksi mikroaaltouuni sekä bluetooth-laitteet aiheuttavat 2,4 GHz:n taajuusalueella. 5 GHz:n alueella kanavien varaama kaista on huomattavasti leveämpi, jolloin myös suorituskyky on huomattavasti korkeampi. 802.11a standardissa päällekkäisistä kanavista aiheutuva interferenssi on minimaalinen tai lähes olematon. Haittapuolina ovat lähinnä laitteiden huono saatavuus, hinta sekä heikompi katealue ja läpäisykyky johtuen tiheämmästä aaltopituudesta. (Geier 2005, 125.)

IEEE ratifioi myös **802.11b-standardin** samaan aikaan 802.11a-standardin kanssa. 802.11b toimii 2,4 GHz:n taajuusalueella 1, 2, 5,5 tai 11 Mbps:in datasiirtonopeudella käyttäen DSSS-tekniikkaa ja lisäksi CCK-modulointia. (Geier 2005, 126.) Standardin todellinen lähetysnopeus on kuitenkin noin 5 Mbps (Jaakohuhta 2005, 268). Merkittävä etu A-standardiin verrattuna on huomattavasti suurempi kantama, mutta B:n haittapuolena on kanavien päällekkäisyys. 2,4 GHz:n taajuusalueella on vain kolme suositeltavaa toisiaan häiritsemätöntä kanavaa (Euroopassa kanavat 1, 7 ja 13). Taajuusalueen ollessa 2,4 GHz on yleistä törmätä RF-interferenssiin, sillä mikroaaltouunit

sekä langattomat puhelimet käyttävät kyseistä taajuutta. (Geier 2005, 126–127.)

802.11g on IEEE:n ratifioima laajennus vuodelta 2003. Toiminnaltaan 802.11g on identtinen 802.11a:n kanssa, eroten vain taajuusalueeltaan. Tiedonsiirtonopeus on maksimillaan 54 Mbps OFDM-tekniikan avulla. Todellisuudessa standardin lähetysnopeus vastaa 32 Mbps. 802.11g on yhteensopiva 802.11b:n kanssa. Haittapuolena on kuitenkin datasiirtonopeuden laskeminen 802.11b:n tasolle, jos verkossa on yksikin laite, mikä ei tue g-standardia. Tämä johtuu standardien käyttämien modulointitekniikoiden eroavaisuuksista. (Granlund 2007, 305; Jaakohuhta 2005, 268.)

IEEE aloitti **802.11n-standardin** kehitystyön vuonna 2004, jonka tavoitteena oli kehittää standardi toimimaan 200–540 Mbps:in datasiirtonopeudella. Toisena tavoitteena oli myös kasvattaa katealuetta noin 50 prosentilla. Tämä on mahdollista MIMO-antennitekniikan (Multiple Input Multiple Output) avulla. Tarkoituksena on siis käyttää useampaa antennia, jolloin jokainen antennipari käsittelee omaa lähetettään. Kaistanleveysvaihtoehtoina on 20 tai 40 MHz:iä. (Granlund 2007, 305.)

Muita IEEE:n standardipäivityksiä on kehitteillä tasaisin väliajoin, joista vain osa päätyy lopulliseksi standardiksi. Taulukko 1 kuvastaa IEEE:n lähiverkkostandardien lisämääritelmiä.

Taulukko 1. IEEE 802.11-standardin laajennukset (soveltaen Rackley 2007, 140–141)

Standardinimike	**Ominaisuus**
802.11d	MAC-tasoisen konfiguroinnin taajuuksiin, virran asetuksiin sekä signaalin kaistanleveyteen vastaamaan paikalliseen radiosignaalien säädöksiä, helpottaen näin kansainvälistä roaming-mahdollisuutta.
802.11e	Verkon suorituskyvyn ja palvelulaadun parantamiseen liittyviä päivityksiä. (Quality of Service, QoS)

802.11h	Spektrin hallinta 5 GHz:n taajuusalueelta. Sisältää dynaamisen taajuuden valinnan (DFS) sekä lähetystehon hallinnan (TCP). Tarkoituksena vähentää häiriötekijöitä Euroopan alueen asevoimien tutka- ja satelliittikommunikoinnissa.
802.11i	Sisältää tietoturvapäivityksiä autentikointiin sekä salaukseen. Mahdollistaa AES-salauksen käyttämistä sekä 802.1x-autentikointia.
802.11j	Japaniin kohdistettu aluepäivitys 802.11a-standardiin. Lisää radiokanavia 4.9 – 5.0 GHz:n välille.
802.11k	Mahdollisuus optimoida verkon tehokkuutta kanavavalintojen, roaming:in sekä TCP:n kautta. Tehokkuutta kasvatetaan selvittämällä kaikki alueella toimivat tukiasemat (myös heikompi signaaliset).
802.11p	Mahdollisuus liikkuvien ajoneuvojen välisen kommunikoinnin (WAVE). Mahdollisti myös kommunikoinnin ajoneuvon ja paikallaan olevan tukiaseman välillä. Käyttää Intelligent transportation system-tekniikkaa (ITS) 5.9 GHz:n taajuusalueella.
802.11r	Tarjoaa nopean siirtymän mobiililaitteille kahden BSS-verkon välillä mahdollistaen VoIP-puhelut tukiaseman vaihdoksen yhteydessä.
802.11s	802.11 MAC-kerroksen laajennus mahdollistaen ESS solmuverkot.
802.11u	Lakimuutos fyysiseen- ja MAC-tasoon mahdollistaen tiedonsiirron muidenkin kuin 802.11-standardien välillä (Bluetooth, ZigBee, WiMAX).
802.11v	Lisää suoritustehoa, vähentää interferenssiä sekä lisää luotettavuutta verkkohallinnan kautta.
802.11w	Tietoturvalisäys hallitsemismahdollisuuksista datakehyksiin.

2.9.3 HiperLAN/2

Kilpaileva langattoman lähiverkon standardi on ETSI:n (European Telecommuniactions Standards Institute) kehittämä HiperLAN (High Performance Radio LAN). HiperLANin ensimmäinen versio tarjosi 20 Mbps datasiirtonopeuden 5 GHz:n vapaasti käytettävällä taajuusalueella IBSS-verkossa. Standardin seuraava versio HiperLAN/2 toimii samalla taajuusalueella kuin edeltäjänsä, mutta tarjoaa 54 Mbps siirtonopeuden käyttäen OFDM-monikantoaaltomodulointia. Standardi sisältää myös 802.11e:n kaltaisen QoS-palvelun. HiperLANin kolmas versio oli nimeltään HomeRF. Nimensä mukaisesti standardi oli tarkoitettu kotikäyttöön, johtuen lyhyistä yhteysväleistä. HomeRF:ia ei ole enää tarjolla ja laitteiden valmistus on lopetettu. (Puska 2005, 47–48.)

ETSI:n kehittämä tekniikka ei kuitenkaan ole saanut tarvittavaa kannatusta tullakseen todelliseksi uhaksi IEEE:n standardille. HiperLAN-tekniikkaa tukevia laitteita markkinoilla löytyy hyvin vähän. HiperLAN:ia ei käsitellä tässä opinnäytetyössä sen tarkemmin, sillä kyseistä tekniikka ei tulla käyttämään Santapark Oy:ssä.

3 LANGATTOMAN VERKON TIETOTURVA

3.1 Tietoturvan tavoitteet

Langattoman lähiverkon tietoturva on vähintäänkin yhtä tärkeää, ellei jopa tärkeämpää kuin normaalissa Ethernet-verkossa. Tieto liikkuu ilmateitse, minkä takia datakehysten liikerataa ei pystytä hallitsemaan yhtä helposti kuin kaapeliratkaisulla. On mahdollista, että ulkopuolinen taho pääsee datakehyksiin käsiksi jos tietoturva ei ole riittävän korkealla tasolla.

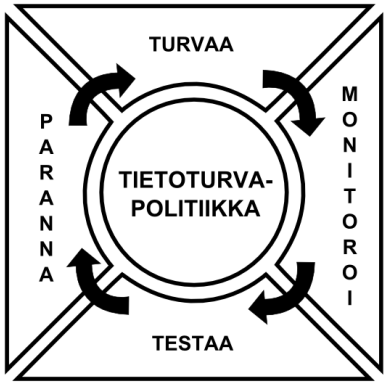
Langattoman lähiverkon tietoturvaan on hyvä soveltaa IETF:n (Internet Engineering Task Force) kehittämää tietoturvapalvelulistaa. Turvapalveluita on yhteensä kuusi ja jokainen listaan kuuluva palvelu täydentää toinen toistaan (taulukko 2). (Puska 2005, 70.)

Taulukko 2. Tietoturvapalvelulista (soveltaen Puska 2005, 70)

1.	Tiedon luottamuksellisuus (Confidentiality)	Tietoja tai dataa voidaan selata, lukea ja välittää vain siihen oikeutetut henkilöt.
2.	Tiedon eheys (Integrity)	Tiedon muokkaaminen ja poistaminen on mahdollista toteuttaa vain siihen oikeutettu henkilö. Eheys koskee tiedon syöttöön, tallentamiseen, käsittelyyn ja siirtoon.
3.	Todennus (Authentication)	Tehdyt muutokset tietoon voidaan todentaa myös jälkikäteen.
4.	Kiistättömyys (Non-repudiation)	Tiedon, henkilöstön sekä toimenpiteiden aitouden ja eheyden varmentaminen.
5.	Pääsynvalvonta (Access Control)	Oikeutettujen henkilöiden todentaminen.
6.	Käytettävyys (Availability)	Tieto on käsiteltävissä siihen oikeutettavilla henkilöillä sovittuun aikaan kaikissa olosuhteissa.

Langattoman lähiverkon tietoturvatyö on jatkuvaa. Järjestelmällinen tietoturvatyö takaa luotettavan ja turvallisen verkon sekä mahdollistaa ongelmatilanteista selviytymisen. Kuvio 11 esittää ihanteellista tietoturvapolitiikkaa verkkotietoturvan suhteen. Langattoman lähiverkon tietoturvatyötä on kuitenkin hyvä tarkentaa langattoman tiedonsiirron merkityksen mukaan. Ei ole kannattavaa palkata tietoturvatyöstä vastaavaa henkilöstöä huolehtimaan langattomasta siirtotiestä, jossa tapahtuva liikenne on hyvin rajattua ja tärkeimmät palvelut ovat parikaapelin välityksellä Ethernet-verkossa.

Suositeltavaa on, että tietoturvatyö olisi jatkuvaluonteista työtä, sillä hyvin harvoin kerran asennettu tietoturvaratkaisu on luotettava. Ajan myötä tekniikka kehittyy sekä turvallisuuden puolesta että sitä vastaan. Tästä syystä tietoturva on suositeltavaa pitää päivitettynä.



Kuvio 11. Jatkuvaluonteinen tietoturvapolitiikka (Puska 2005, 71)

Langattoman lähiverkon laitteiden fyysinen tietoturva on tärkeää. Laitteet on hyvä sijoittaa paikkoihin, joissa ne ovat suojassa ulkopuolisilta. Tällä tavoin verkkolaitteen portteihin ei ole mahdollista liittää siihen tarkoittamattomia laitteita. (Puska 2005, 71.) Laitteen oletus-salasana on myös vaihdettava vaikeasti arvattavaan ja hakkeroitavaan salasanaan, joka sisältää numeroita, isoja alkukirjaimia. Erikoismerkkejä on myös suositeltavaa käyttää salasanoissa, jos vain on mahdollista.

3.2 Uhat

Langattomassa viestinnässä tietoturvan tarve on elintärkeää, sillä suojaamattoman verkon signaaleja voi kuka tahansa ulkopuolinen käyttää hyväkseen ja pahimmassa tapauksessa luottamuksellisia tietoja voi joutua ulkopuolisten käsiin. Langattomiin lähiverkkoihin kohdistuu monenlaisia uhkia. Näistä yleisimpiä ovat niin sanottu passiivinen tarkkailu, luvaton pääsy, palvelunesto sekä välistävetoyritykset.

3.2.1 Passiivinen tarkkailu

Passiivisella tarkkailulla tarkoitetaan langattoman lähiverkon verkkoliikenteen tarkkailua. Uhka on varteenotettava varsinkin suojaamattomassa verkossa, sillä henkilön ei tarvitse olla yrityksen tiloissa päästäkseen yrityksen verkkoon käsiksi. Tarkkailu on myös vaara heikosti suojatuissa verkoissa, sillä heikot salausavaimet on mahdollista purkaa vaivattomasti Internetistä löytyvien ohjelmistojen avulla.

Passiivista tarkkailua voi tapahtua myös pitkien matkojen päästä suunnattavan antennin avulla. Suunta-antennin kautta tapahtuvaa passiivista tarkkailua ei voida havaita, joten paras vaihtoehto on suojautua siltä. (Puska 2005, 69.) Passiiviselta tarkkailulta on mahdollista suojautua käyttämällä riittävän turvallista salausprotokollaa tai karsimalla kuuluvuusaluetta. Lisää ohjeita suojautumiseen löytyy osioista 3.3 Suojautuminen.

3.2.2 Palvelunesto (DoS)

Palvelunestohyökkäys voi hidastaa tai kaataa langattoman verkon. Suojautuminen DoS-hyökkäyksiä vastaan on aina tärkeää langattomissa verkoissa, oli kyse sitten yrityksestä tai kotikäyttäjästä. Pahimmat seuraukset palvelunestosta ovat usein yritystiloissa, joissa langaton verkko on keskeinen osa verkkotoimintaa, kuten langattomassa varastonhallintajärjestelmässä. Tällaisessa tilanteessa langattoman verkon toimimattomuus voisi aiheuttaa huomattavia taloudellisia tappioita. (Geier 2005, 176.)

Palvelunestohyökkäysten muotoja on useita. Näistä yksi toimintatapa on väsytyshyökkäys. Siinä verkko väsytetään valtavalla määrällä turhia paketteja, jolloin verkon resurssit kulutetaan ja seurauksena verkko voi kaatua. Toinen keino on voimakkaiden radiosignaalien käyttö, jotka häiritsevät ja lamauttavat kohteen langattoman verkon. Tähän hakkeri tarvitsee tehokkaan lähettimen, jonka sijainti voidaan analysoida paikannusvälinein. DoS-hyökkäykset käyttävät myös WLAN-verkon tietoturvamekanismeja hyödykseen. WPA-tunnistautumistekniikkaa käyttävä lähiverkko on mahdollista kaataa, kun ulkopuolisesta suunnasta lähetetään kaksi valtuuttamatonta pakettia sekunnin sisällä. WPA olettaa joutuneensa hyökkäyksen kohteeksi ja käynnistää verkon uudelleen. (Geier 2005, 176–177.)

Palvelunesto voi tapahtua myös tahattomasti, sillä 2,4 GHz:n taajuusalueella toimivat lähiverkot toimivat samalla taajuusalueella mikroaaltouunien, bluetooth-laitteiden, langattomien puhelimien sekä ympäristössä toimivien muiden langattomien verkkojen kanssa. Tästä voi aiheutua RF-interferenssiä. (Geier 2005, 177.) Tahattomat palvelunestot voidaan estää vaihtamalla langattoman verkon käyttämää taajuuskanavaa tai vaihtamalla tukiaseman lähettämää taajuusaluetta korkeammalle. Taajuusalueen nostaminen vaatii kuitenkin uuden verkkolaitteen hankinnan, sillä harva WLAN-tukiasema ymmärtää molempia taajuusalueita.

3.2.3 Välistävetohyökkäys

Välistävetohyökkäyksessä hakkeri asettaa kohteensa langattoman verkon ja käyttäjän väliin luvattoman laitteen tai niin sanotun rosvolaitteen. Tällä tavoin hakkeri saa ohjattua kaiken liikenteen pääteaseman ja käyttäjän välillä kulkemaan oman laitteensa kautta, jolloin hakkeri pääsee käsiksi lähetettyyn dataan. Välistävetohyökkäys käyttää apunaan TCP/IP-verkoista tuttua ARP-protokollaa. ARP selvittää kohdeverkkokortin fyysisen osoitteen. Onnistuneen välistävetohyökkäyksen avulla hakkeri voi päästä käsiksi yrityksessä käytössä oleviin salasanoihin tai pahimmassa tapauksessa muodostaa yhteyden yrityksen palvelimiin kenenkään huomaamatta. (Geier 2005, 174–175.)

Välistävetohyökkäyksiä vastaan on tarjolla Secure ARP -tekniikka (SARP). SARP muodostaa niin sanotun turvatunnelin tukiaseman ja asiakkaan välille. SARP hylkää kaikki tunnelin ulkopuolelta tulleet pyynnöt, joten välistävetohyökkäys on mahdotonta. Secure ARP vaatii kuitenkin erillisen ohjelmiston asentamisen jokaiselle laitteelle erikseen. (Geier 2005, 175–176.) Tästä syystä tekniikkaa ei ole käytännöllistä käyttää vapaissa ja usein muuttuvissa verkoissa.

3.3 Suojautuminen

Suojautuminen langattomaan lähiverkkoon kohdistuneilta hyökkäyksiltä on moniosainen ja tasoinen prosessi. Tietoturvatyön voidaan ajatella alkavan jo rakennuksen suunnitteluvaiheessa, sillä yksi hyvin tehokas suojautumistapa on signaalin ulkopuolelle leviämisen- ja ulkopuolisten radiosignaalien sisäänantulon estäminen. Tämän toteuttaminen jälkikäteen on haasteellista.

Ikkunoihin kohdistetut rakenneratkaisut estävät signaalin läpäisykyvyn. Tästä syystä ikkunoiden tulisi olla kuparilämpöeristettyjä tai vaihtoehtoisesti metallikalvopohjaisia. Ikkunoiden kaihtimia tulisi välttää ja sen sijaan käyttää metallivärjäystä. Seinärakenteet on huomioitava ja sisäseinän metallisten tukirakenteiden maadoitus on varmistettava. Sisä- ja ulkoseinissä on suositeltavaa käyttää metallipohjaisia maaleja. Signaalien läpäisykykyä on tarpeellista tutkia, jolloin saadaan kokonaiskuva signaalin vuotamisesta rakennuksen ulkopuolelle. Tätä pystytään minimoimaan suuntaamalla tukiasemien antennit rakennuksen sisäosan suuntaan. (Geier 2005, 177–178.) Vaihtoehtoina markkinoilta löytyy myös radiosignaaleja estäviä maaliratkaisuja.

Rakennukseen kohdistuvat tietoturvaratkaisut on suositeltuja ottaa harkintaan rakennuksen valmistusvaiheessa. Jälkikäteen kyseiset ratkaisut ovat haastavia ja usein kalliita toteuttaa. Onkin suositeltavaa käyttää vaihtoehtoisia tietoturvaratkaisuja, jos rakennukseen kohdistuva tietoturva on puutteellista. Rakennuksen tietoturvallisen rakentamisen lisäksi on erittäin suositeltavaa käyttää radiosignaalin salausta sekä käyttäjäkohtaisten avainten avulla tapahtuvaa autentikointia.

3.3.1 MAC-suodatus

Langattoman verkon liikennettä on mahdollista rajata MAC-suodattimen avulla, jolloin WLAN-tukiasemalle pääsevät vain laitteet, jotka ovat määriteltynä tukiaseman MAC-osoite -listassa. MAC-suodatusta ei suositella yritysmaailmassa, sillä pitkien heksadesimaalisten MAC-osoitteiden listaaminen ja ylläpito on työlästä ja aikaa vievää. (Puska 2005, 73.)

MAC-suodatus ei ole myöskään täysin turvallinen ratkaisu, sillä useat verkkourkintaan tarkoitetuista ohjelmista näyttävät myös verkkoon liitettyjen verkkolaitteiden MAC-osoitteet. Hakkerin on mahdollista vaihtaa oman verkkolaitteensa MAC-osoite vastaamaan luvallisen käyttäjän osoitetta ja tällä tavoin päästä käsiksi verkkoon. MAC-suodatus toimii parhaiten kotikäytössä tai pienissä yrityksissä, joissa uusia verkkolaitteita tulee käyttöön harvoin. (Geier 2005, 187.)

3.3.2 WEP

Wired Equivalent Privacy on 802.11-standardeista löytyvä, mutta hyvin harvoin suositeltava suojaustekniikka. WEP:in kehitysvaiheessa tarkoituksena oli tuoda salaustekniikka, joka vastaisi normaalia Ethernet-lähiverkon turvallisuutta. Nykypäivänä ei ole suositeltavaa käyttää WEP-salausta langattomissa verkoissa, sillä tarjolla on huomattavasti turvallisempia vaihtoehtoja.

WEP käyttää salaamiseen symmetristä, kaikille laitteille samaa salausavainta. Ilman oikeaa avainta, verkkolaite ei pääse liittymään salattuun verkkoon. Vaihtoehtoina on 64-bittinen ja myöhemmin tietoturvaa lisäämään tuotu 128-bittinen salausavain, jonka turvallisuus edelliseen versioon verrattuna jäi lähinnä kosmeettiselle tasolle. Molemmat salausavaimet sisältävät 24-bittisen alustusvektorin (Initialization Vector). Tietoturvallisesti molemmat avaimet ovat kuitenkin haavoittuvaisia, sillä salasanan symmetrisyyden takia ulkopuolinen verkkokuuntelija voi saada selville salausavaimen keskimäärin neljällä miljoonalla lähetetyllä datakehyksellä. (Rackley 2007, 209.)

3.3.3 WPA/WPA2

Wi-Fi Alliance kehitti Wi-Fi Protected Access -salaustekniikan, tarkoituksenaan parantaa suojautumista kohdistettuja hyökkäyksiä vastaan WEP:in epäonnistuessa siinä. WPA on mahdollista saada verkkolaitteeseen pelkän firmware-päivityksen avulla. (Granlund 2007, 320.)

WPA1 käyttää salausavainten hallintaan Temporal Key Integrity Protocol -tekniikkaa (TKIP) ja tarjoaa mahdollisuuden 802.1x-autentikointiin käyttäen EAP (Extensible Authentication Protocol)-pakettisuodatusta ulkopuolisen palvelinratkaisun kautta. Vaihtoehtona 802.1x-autentikoinnille on PSK (Pre-Shared Key)-salausavain, jolloin ulkopuolista palvelinta ei tarvita. (Rackley 2007, 212.) PSK-salausavainta käytettäessä tukiasema ja asiakas todentavat toisensa haaste-vastaus–tekniikalla (eng. Challenge-response) käyttäen molempien tuntemaa salausavainta (eng. Master Key) (Granlund 2007, 320). WPA:n versio 2 (WPA2) lisäsi salausavaimen hallintaan liittyvää tietoturvaa AES-salauksella (Advanced Encryption Standard) (Rackley 2007, 212).

3.3.4 TKIP

Temporal Key Integrity Protocol eli TKIP on eräs 802.11-standardin päivityksistä, joka sisältää joukon algoritmeja, joiden tarkoituksena oli korjata WEP:in tietoturvaa erityisesti salasanan muodostamisessa. Kehyskohtainen 128-bittinen salausavain poistaa WEP:issä olleen salasanan uudelleenkäytön ongelmat. (Geier 2005, 183.)

> ”TKIP:in osapuolet aloittavat salauksen yhteisellä 128-bittisellä aloi tusavaimella (Temporal Key), joka yhdistetään työaseman MAC-osoitteeseen ja kehyksen järjestysnumeron neljään eniten merkitse vään bittiin. Saatu väliaikainen avain yhdistetään järjestysnumeron kahteen alimpaan bittiin, jonka tuloksena on kehyskohtainen avain.” (Puska 2005, 82.)

Kehyskohtainen avain on jokaiselle laitteelle uniikki. TKIP vaihtaa satunnaisavaimia viimeistään 10 000 lähetetyn paketin jälkeen, riippuen tietoturva-

vaatimuksista. Salakuuntelijoille ei anneta mahdollisuutta kerätä riittävästi dataa avaimen purkamista varten. (Geier 2005, 183.)

3.3.5 AES

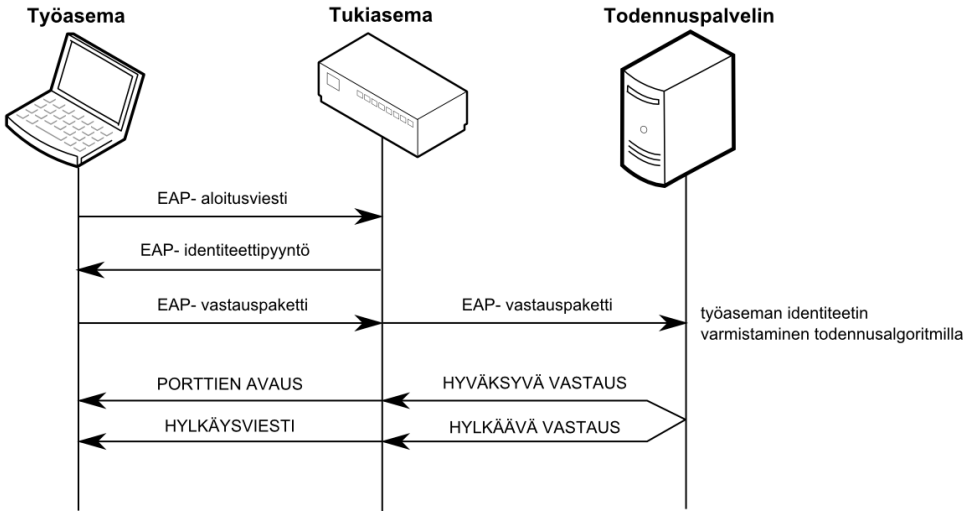
Advanced Encryption Standard eli AES tarjoaa TKIP:iä huomattavasti vahvemman salauksen. AES on symmetrinen salausalgoritmi, joka käsittelee dataa 128 bitin lohkoina. Symmetrisyys tarkoittaa sitä, että tiedon salaamiseen ja purkamiseen käytetään samaa avainta. Protokolla on saanut Yhdysvaltojen hyväksynnän, ja se on käytössä liittovaltioiden salausprotokollana. AES-salattua tiedostoa on mahdotonta purkaa ilman salausavainta. Ainoa mahdollinen tapa saada selville salausavain on niin sanottu brute-force -hyökkäys, jolloin käydään jokainen mahdollinen salausavain läpi. Tämä on kuitenkin epätodennäköistä, sillä teoreettisesti jokainen ylimääräinen bitti salausavaimessa tuplaa algoritmin vahvuuden. (Seleborg 2007, 1–2.)

Teoriassa jos tiedoston salaamiseen käytetään 128-bittistä AES-salausta ja käytössä on tietokone, jolla voidaan testata biljoona avainta sekunnissa, tietokoneelta veisi yhteensä noin 10 000 triljoonaa vuotta, ennen kuin avain saadaan selville. Salaamiseen voidaan käyttää 128, 192 tai 256 bitin salausavainta. AES-salausta käytettäessä on tärkeää käyttää vaikeasti arvattavaa salasanaa, sillä heikolla salasanalla varustettu AES ei ole turvallinen. (Seleborg 2007, 3.)

3.3.6 802.1x-todennus

802.1x-tunnistuksen perusidea on yksinkertainen. Tunnistamaton asiakas pyrkii muodostamaan yhteyttä langattomaan tukiasemaan. Tukiasema avaa asiakkaalle portin, jossa on sallittua vain EAP-pakettien (Extensible Authentication Protocol) lähettäminen. Asiakkaan tunnistamisen jälkeen tukiasema avaa asiakkaan loput portit ja mahdollistaa muun muassa http-, DHCP- ja POP3-pakettien lähettämisen. 802.1x-protokolla tarjoaa tehokkaan tietoturvan, vaikka WLAN-verkossa olisi käytössä WEP-salaus tai ei salausta ollenkaan. (Geier 2005, 189–190.)

802.1x-tunnistustekniikka on hyvin turvallinen ratkaisu yrityksen langattomaan verkkoon. Kuviossa 12 työasema lähettää tukiasemalle EAP-aloitusviestin, johon tukiasema vastaa EAP-identiteettipyyntöviestillä. Työaseman vastatessa pyyntöön identiteetin sisältävällä EAP-vastauspaketilla, todennuspalvelin käyttää todennusalgoritmia asiakkaan identiteetin selvittämiseen. Oikeutetun käyttäjän portit avataan ja asiakas pystyy käyttämään verkkoa ja vastaavasti hylkää asiakkaan, jos identiteetti ei ole oikea. (Geier 2005, 189–190.)



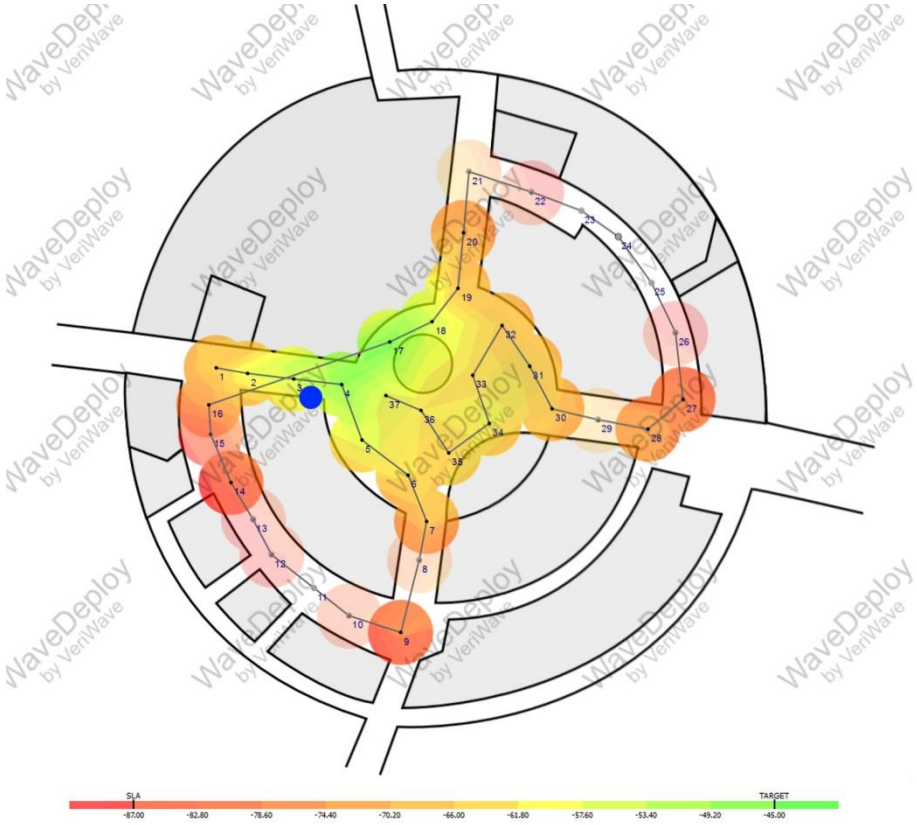
Kuvio 12. 802.1x-todennus

4 SANTAPARK OY:N VERKKOSUUNNITELMA

4.1 Nykytilanne

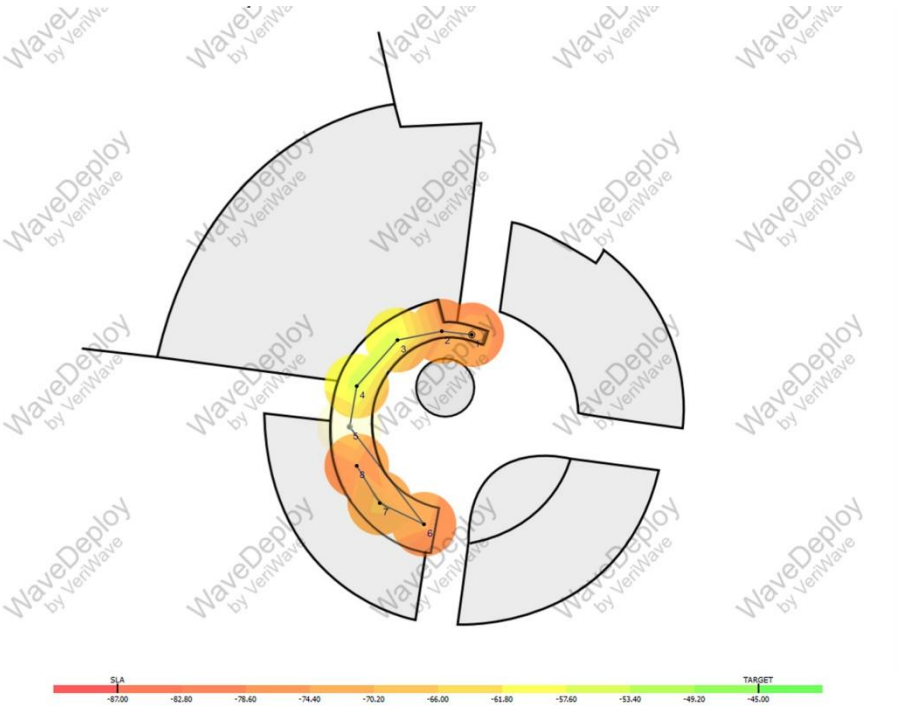
Santaparkissa on käytössä yksi WLAN-tukiasema asiakkaiden käyttöön, sekä yksi Apple-tietokonevalmistajan tuottama tukiasema toimistossa yrityksen työntekijöitä varten. Molemmat nykyiset käytössä olevat laitteet ovat kytkettynä samaan kytkimeen ja reitittimeen. Lähiverkkouudistuksen tarkoituksena on lisätä tukiasemien määrää ja optimoida laitteet toimimaan ongelmitta.

Asiakkaiden käyttöön varattu tukiasema sijaitsee yrityksen tiloissa olevan kahvion läheisellä käytävällä (Kuvio 13, kahvio esitetty kuvassa sinisenä ympyränä), josta on suora näköyhteys vain osaan kahviosta. Tukiasemassa on käytössä DHCP-palvelin ja käytettävä taajuusalue on 2,4 GHz:iä. Kahvio sijaitsee keskellä Santaparkkia ja on malliltaan rakennuksen pohjapiirroksessa sivultapäin kuvattuna puolipallo ja ylhäältä kuvattuna täysi ympyrä. Myyntitiski sijaitsee lähellä kahvion keskikohtaa ja näkyy mallikuvassa kahvion sisällä olevana pienempänä pyöreänä ympyränä.



Kuvio 13. Santapark WLAN-tukiasema kahvion pöydällä

Kahvion ruokailutiloja on myös yläparvella (Kuvio 14), jossa sijaitsee myös DJ:n työpiste (ei ole merkittynä kuviossa). Kuvioista 13 ja 14 on nähtävissä, että kuuluvuus on heikkoa suurimmassa osassa kahvioaluetta (Kuvioiden informaatiografiikassa vihreä väri merkitsee vahvaa signaalia, punainen heikkoa). Kuuluvuus oli hyvää vain tilanteissa, joissa käytettävä laite on suorassa näköyhteydessä tukiasemaan. Kahvioalueen yläparvella kuuluvuus oli erittäin heikkoa. Yläparvelta löytyi kohtia, joissa verkkoa ei tunnistettu lainkaan.



Kuvio 14. Santapark WLAN-tukiasema yläparvella

Nykypäivänä myös yleisillä paikoilla on hyvin tavallista selailla Internetiä ruokailun tai kahvitauon yhteydessä. On siis tärkeää asiakkaiden viihtyvyyden ja asiakastyytyväisyyden kannalta parantaa kuuluvuutta sekä tarjota katkeilematon Internet-yhteys asiakkaille.

4.2 Suunnitelma

Työtehtäviini kuului kahvioalueen sekä asiakkaiden käyttöön varattujen tilojen WLAN-toteutus sekä yrityspuolen WLAN-ratkaisut. Painoarvo verkkojen suhteen oli kuitenkin asiakkaiden langattomassa verkossa. Santaparkin verkko tullaan yrityksen vaatimusten mukaan jakamaan yritysverkkoon ja asiakasverkkoon. Tällä tavoin asiakasverkosta ei ole mahdollista päästä käsiksi yri-

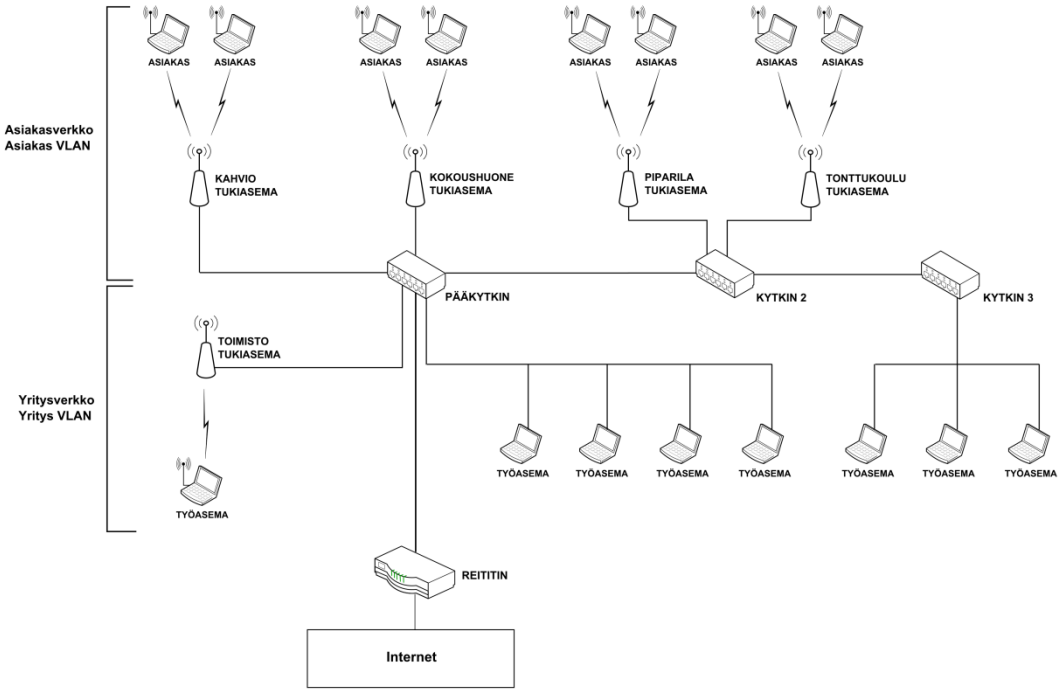
tyspuolen laitteisiin ja näin vaarantaa yrityksen sisäinen tietoturva. Verkon jakaminen tapahtuu Virtual LAN (Virtual Local Area Network, VLAN) -tekniikalla, koska VLAN ratkaisun hyötyinä on sen helppo ja nopea asentaminen ja konfigurointi.

Yksinkertaistettuna VLAN:in tarkoitus on mahdollistaa yhden kytkimen toiminta vastaamaan usean kytkimen tarjoamia palveluita. Tämä vähentää verkkolaitteiden määrää yrityksessä ja helpottaa kaapelien asentamista ja verkon hallintaa. Tulevaisuudessa mahdolliset muutokset on myös nopea suorittaa. VLAN:in avulla pystytään verkko jakamaan omiin loogisiin osiin (virtuaalisiin lähiverkkoihin). Tämä tapahtuu kytkimen porttikohtaisissa asetuksissa, joissa määritellään, mihin VLAN ryhmään/ryhmiin porttiin kytkettävä laite kuuluu. Yksi kytkimistä toimii pääkytkimenä verkolle. Pääkytkin on usein yhdistettynä reitittimeen. VLAN konfiguroidaan kaikkiin kytkimiin niin, että liikenne eri kytkinten VLAN:ien välillä on mahdollista. Jokaiseen kytkimeen on asennettava samat VLAN:it ja niiden VLAN ID:t (Virtual LAN Identifier) on vastattava toisiaan.

Santapark toteutuksessa tullaan käyttämään kolmea VLAN ryhmää: Hallinto VLAN, Yritys VLAN ja Asiakas VLAN. Hallinto VLAN:iin kuuluvat vain tietyt työpisteet, jotka toimivat niin sanottuina terminaaleina verkon hallintaan. Yritys VLAN:in tulee sisältää kaikki yrityksen työntekoon vaadittavat verkkolaitteet (muun muassa tulostimet ja kassalaitteet). Asiakas VLAN:in tarkoituksena on jakaa asiakaskunnalle Internet yhteys. Asiakas VLAN-portteihin kytketään asiakaskäyttöön varatut tukiasemat, jotka jakavat verkkoa eteenpäin radiosignaalien avulla. Eristettynä omaan virtuaalilähiverkkoonsa asiakkailla ei ole mahdollisuutta päästä käsiksi yritysverkkoon tai hallintoverkkoon. Yritysverkko ja asiakasverkko tulevat käyttämään omaa IP-osoitteistoa. Esimerkiksi yrityksen työntekijöille varattu verkko käyttää 10.16.60.X-alkuisia osotteita ja asiakkaiden verkko käyttää 10.16.70.X-alkuisia osoitetta.

Kytkimeen asennetaan Trunking-toiminto, jonka avulla kytkinten välinen VLAN-liikenne mahdollistetaan. Lähetettävään datakehykseen lisätään VLAN ID, jonka avulla kytkin pystyy tekemään tarvittavat toimenpiteet oikean osoitteen saavuttamiseksi. Santaparkissa Trunking tullaan toteuttamaan valokaa-

pelin avulla. Kuviossa 15 esitetään selkeämpi kuva verkkorakenteesta. Yritysverkon puolelle kuuluvat myös oheislaitteet ja kassajärjestelmät, joista ei turvallisuussyistä tässä tutkimuksessa kerrota enempää.



Kuvio 15. Santapark verkkosuunnitelma

Rakennuksesta ei ole lupaa käyttää tarkkaa pohjapiirrosta tässä yhteydessä, joten suunnitelmaa varten toteutin piirroksen, josta näkyvät tälle suunnitelmalle oleelliset verkkoalueeseen kuuluvat huoneet. Kahvioalueen langaton verkko tullaan alustavasti toteuttamaan yhdellä tukiasemalla, mutta otin myös tulevaisuuden varalle mahdollisuuden Roaming-tekniikkaan.

4.3 Asiakasverkko

4.3.1 Kahvioalueen kuuluvuuden mittaaminen ja arviointi

Aloitin alueen tutkimisen verkkosuunnitelman toteuttamista varten kuuluvuuden mittaamisella ja sen kartoittamisella. Tällä tavoin sain selvitettyä tukiasemalle parhaan mahdollisen sijainnin. Kuuluvuuden mittaamiseen käytin Applen kannettavalle tietokoneelle asennettua AirRadar-ohjelmistoa sekä Android-käyttöjärjestelmälle kehitettyä Wi-Fi Analyzer -ohjelmaa. Lopullisen

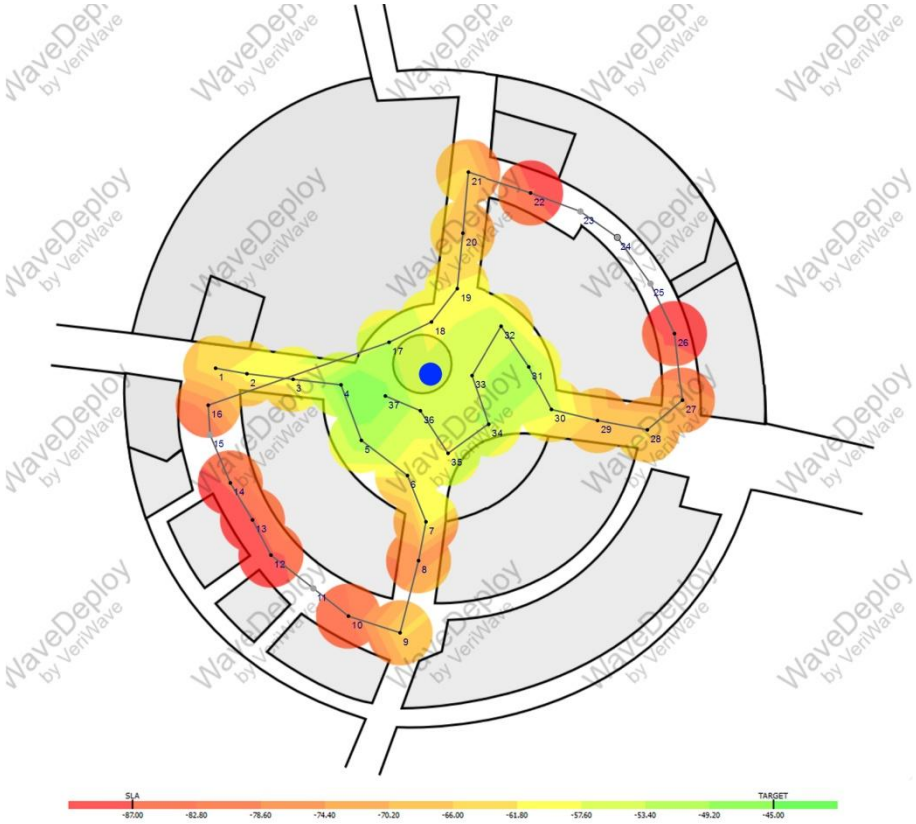
kartan kuuluvuudesta toteutin kuitenkin VeriWave:n kehittämällä WaveDeploy Basic -ohjelmistolla. Ohjelman ilmainen versio on kuitenkin rajoitettu vain mahdollisen latausnopeuden tarkkailuun. Koska tämän projektin yhtenä päämääränä oli toteuttaa suunnitelma mahdollisimman taloudellisesti, valitsin ilmaisen version. WaveDeploy Basic -ohjelman antamat tulokset palvelivat hyvin suunnitelman tarpeita.

WaveDeploy Basic käyttää apunaan rakennuksen pohjapiirrosta. Pohjapiirroksen ei tarvitse olla tarkka, vaan myös suuntaa antava pohjapiirros riittää langattoman verkon tehokkuuden tutkimiseen. Ensin ohjelmaan merkitään aloituspiste, josta kuuluvuusalueen kartoitus aloitetaan. Tärkeää on olla lähellä kartalle merkittyä pistettä. Aluetta kartoittaessani kävelin alueen läpi ja noin kolmen metrin välein päivitin sijaintini ohjelmassa olevaan karttaan. Kuvioissa 13, 14, 16 ja 17 näkyvä, alueen läpi kulkeva ohut musta viiva kuvaa kulkemaani reittiä. Reitin varrella olevat tummat pisteet kuvaavat kohtia, joissa pysähdyin päivittämään sijaintini karttaan. Kulkemani reitti sisälsi kuvioiden keskellä olevan kahvion lisäksi myös sen lähellä olevat käytävät. Ohjelma piirtää näiden kerättyjen pisteiden avulla suuntaa antavan kuuluvuuskartan.

Käytetyt ohjelmat näyttävät alueella olevat langattomat lähiverkot sekä niiden lähettämien signaalien vahvuuden. Käytin signaalien vahvuuden selvittämiseen useita ohjelmistoja, joilla sain selville keskiarvon ja pystyin arvioimaan tulosten paikkansa pitävyyttä. Matkapuhelimen vastaanottokyky oli hieman heikompi kuin kannettavan tietokoneen, johtuen vastaanottimen heikommasta tehosta. Loppujen lopuksi molempien laitteiden tulokset olivat hyvin samankaltaisia, koska niiden välinen vahvuusero oli pieni.

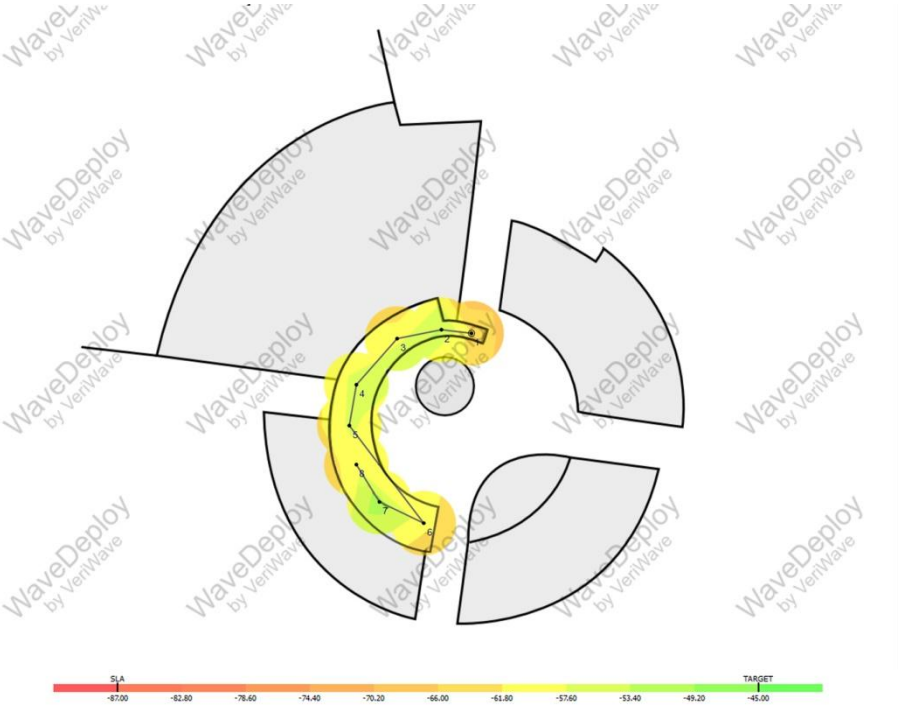
Kuviosta 16 voidaan nähdä, että tukiaseman sijainnilla on huomattava merkitys signaaliin laajuuteen. Asiakaskäytössä olevassa tukiasemassa on kolme ympärille levittyvää antennia, joten tukiasema on parasta sijoittaa mahdollisimman lähelle huoneiston keskiosaa. Asetin testikäytössä olleen tukiaseman kahviomyymälän pöydälle (kuvion 16 sininen ympyrä), minkä seurauksena signaalin laajuus parani huomattavasti. Kuuluvuus oli hyvää yli puoles-

sa pinta-alasta sekä riittävällä tasolla lopulla alueella. Heikkoa kuuluvuutta kahvioalueella ei ilmennyt. Arvioni mukaan kuuluvuuden pitäisi kattaa vähintään 70 prosenttia alueesta hyvällä tasolla, kun tukiasema asetetaan kahvion tiskin läheisyyteen ja sopivalle korkeudelle.



Kuvio 16. Santapark WLAN-tukiasema kahvion pöydällä

On siis selvää, että paras vaihtoehto on siirtää nykyinen tukiasema kahvion tiskin läheisyyteen tai mahdollisesti DJ:n työpisteen läheisyyteen. Signaali on hyvällä tasolla myös yläparvella (Kuvio 17). Tukiaseman kahvion tiskin läheisyyteen asennettaessa on otettava huomioon ympärillä olevat laitteet, sillä työpisteen ympärillä on kahvion ruuanlaitossa käyttämiä paljon lämpöä erittäviä sähkölaitteita. Nämä muut laitteet saattavat pahimmillaan jopa vahingoittaa WLAN-tukiasemaa. Paras vaihtoehto on sijoittaa tukiasema kahvion katokseen sopivalle korkeudelle (n. 1,5–3 metriä). DJ:n työpisteen läheisyyteen asennettaessa ei vaadittaisi liiallisia RJ-45 kaapeliratkaisuja, sillä kopin läheisyydessä on vapaita kytkentärasioita. DJ-työpisteeseen sijoittaessa ulkopuolisilla ei ole pääsyä tukiasemalle. Vaihtoehdoista molemmat ovat varteenotettavia.



Kuvio 17. Santapark WLAN-tukiasema yläparvella

Kahvioalueelle on mahdollista myös asentaa toinen tukiasema, jolloin mahdollistetaan Roaming-tekniikan käyttöä. Kahvion alueella ei ole kuitenkaan aiemmin ilmentynyt verkon ruuhkaantumista, joten Roaming ei ole välttämättömyys.

4.3.2 Kokoushuoneiden kuuluvuuden mittaaminen ja mahdollisuudet

Santaparkin kokoushuoneilla tarkoitetaan kokonaisuuskuvassa näkyviä alueita, jotka yritys on nimennyt seuraavasti: ”Piparila” (huone 1), ”Tonttukoulu” (huone 2) sekä ”Neuvotteluhuone” (huone 3) (ks. Kuvio 18 s. 45). Tilat ovat malliltaan oivallisia kokouksia varten, joten huoneista on oltava yhteys Internetiin. Paras vaihtoehto näihin tiloihin on WLAN-tukiaseman sijoittaminen huoneistoihin, minkä kautta kokoustilassa työskentelevät pääsevät tarvittaessa vaivattomasti Internetiin. Kahvioalueen tukiaseman signaali ei ole tarpeeksi vahva kantamaan yhteenkään kolmesta kokoushuoneesta, joten paras vaihtoehto on asentaa jokaiseen huoneeseen omat tukiasemat. Mittasin myös huoneen 1 ja huoneen 2 alueiden välistä kuuluvuutta käyttämällä testi-

tukiasemaa, mutta rakennuksen paksut seinät estivät signaalin läpäisyn huoneiden välillä.

En pidä hyvänä vaihtoehtona huoneen 1 kautta tulevan signaalin toistamista huoneessa 2, sillä huoneen 1 tukiasema voisi ruuhkautua liikaa. Kokoushuoneiden tukiasemat tulevat olemaan asiakasverkossa, sillä tilat ovat tarvittaessa vuokrattavissa ulkopuolisille asiakkaille. En lisännyt kuvia kokoustilojen kuuluvuusalueista, sillä tukiasema kattaa koko huoneiston erinomaisesti. Testatessa ei ilmennyt minkäänlaisia kuuluvuusongelmia.

4.4 Yritysverkko

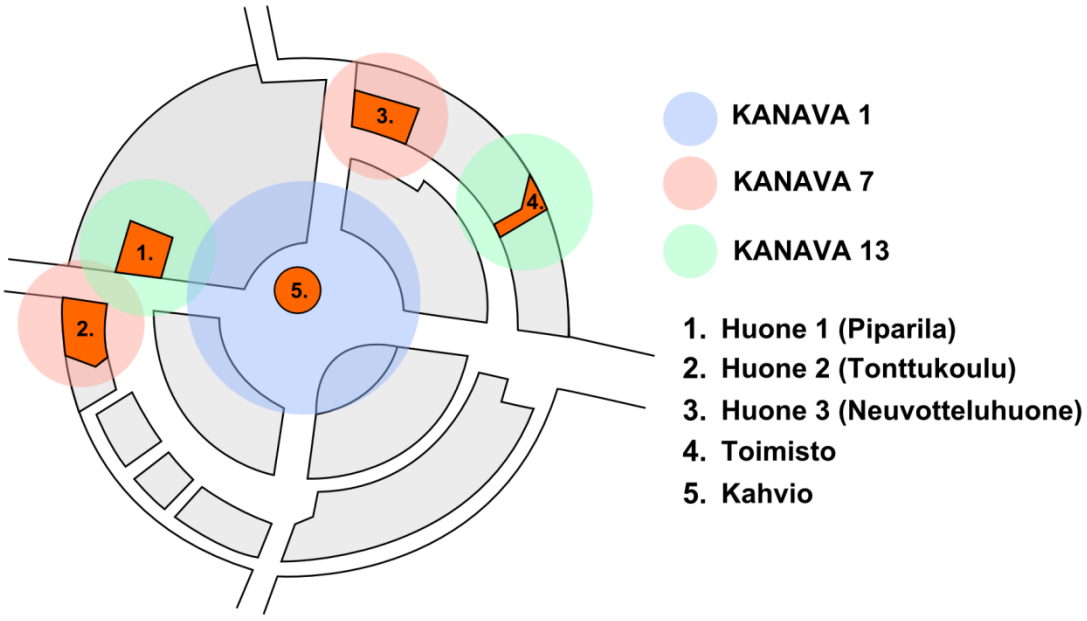
Santaparkin yritysverkko tulee sisältämään kaikki yrityksen laitteet kuten tietokoneet, tulostimet ja kassalaitteet. Yritysverkossa tulee liikkumaan paljon arkaluonteista tietoa, joten se on pidettävä hyvin suojattuna. Yritysverkon topologiaan ei tulla tekemään merkittäviä muutoksia. Yrityspuolelle ei tulla asentamaan useaa WLAN-tukiasemaa tietoturvallisista syistä. Työnteko ei vaadi liikkumista työpisteeltä toiselle, joten yrityspuolen verkkoon liitettyjä tukiasemia tulee vain harkittuihin huoneisiin.

Langaton yritysverkko tulee olla suojattu. Salaustekniikkana suosittelen WPA2 AES-tekniikalla. Autentikointipalvelimelle ei ole tarvetta, sillä langattoman verkon kattama alue on rajallinen, eikä näin pienelle alueelle kohdistettu verkko tarvitse niin korkean tason tietoturvaa.

4.5 Kokonaisuus

Suunnitelman mukaan tukiasemia tulee olemaan viisi tai Santaparkin tarpeiden mukaan vähemmän. Tukiasemat tulevat käyttämään 2,4 GHz:n taajuusaluetta, ja tästä syystä taajuuskanavat on valittava oikein. Standardina käytetään 802.11n- tai g-standardia laitevalinnasta riippuen. Rakennus on pohjapiirroksen mukaan oivallinen useammalle itsenäiselle tukiasemalle, sillä signaali ei leviä laajalle alueelle ja tästä syystä niitä on helppo hallita.

Valitsin jokaiselle tukiasemalle parhaan mahdollisen taajuuskanavan riippuen huoneiston sijainnista. Kahvion tulee käyttää kanavaa 1, sillä se sijaitsee rakennuksen keskellä. Muille huoneistolle jää vaihtoehdoiksi kanavat 7 tai 13. Suosittelen yrityksen toimistossa olevalle tukiasemalle taajuuskanavaa 13. Jos yrityksen laitteet tukevat 5 GHz:n taajuusaluetta on suositeltavaa harkita sen käyttöä. Tällä tavoin kahvion alueen signaalit eivät voi aiheuttaa häiriöitä yritysverkkoon. Yrityksen tukiaseman käyttäessä 2,4 GHz:n taajuusaluetta ei häiriöitä pitäisi ilmetä, sillä kanavat ovat täysin eri puolilla taajuus-spektriä. Huoneelle 2 asennettava taajuuskanava on 7 ja huoneen 1 taajuuskanava on 13. Huoneelle 3 jää vaihtoehdoksi 7, sillä se sijaitsee kohtuullisen lähellä toimistoa ja kahviota. Kuviosta 18 on selkeämpää huomata käytettävät taajuuskanavat.



Kuvio 18. Santapark WLAN-taajuuskanavat

Tukiasemia on mahdollista liikutella kokoustilojen välillä. Jos Santapark päättää olla hankkimatta tukiasemaa esimerkiksi huoneeseen 2, voidaan sinne siirtää tukiasema joko huoneista 3 tai 1. On kuitenkin huomioitava taajuuskanavan vaihto, jos tukiasema päätetään siirtää huoneesta 3, sillä se käyttää samaa taajuutta kuin huone 2. Huoneesta 2 siirto voi tapahtua ilman konfigurointia. Jos kanavien suhteen ilmenee ongelmia on myös mahdollista käyttää automaattista kanavanvalintaa (auto-channel).

Santaparkin tietoturvaratkaisuihin on useita vaikuttavia tekijöitä. Ensimmäinen ja ehkäpä merkittävin tekijä on rakennuksen sijainti ja rakenteelliset ratkaisut. Yritystilat ovat täysin eristettynä muista tiloista, jolloin langattomiin verkkoihin on mahdollista liittyä vain yrityksen sisältä käsin. Paksun kallioseinämän läpi radiosignaalit eivät pääse levittäytymään. Tämä tuo huomattavan tietoturvatekijän tiloihin. Yleisimmät langattomaan verkkoon kohdistuvat uhat ovat epätodennäköisiä, sillä murtautujan on työskentelevä hyvin rajatulla alueella ja aikataululla. Tilojen kulunvalvontaa tarkkaillaan, jolloin ulkopuolisen ei ole mahdollista päästä yrityksen asiakkaille suunnattujen alueiden ulkopuolelle. Käytävillä mahdolliset liitäntäpisteet eivät ole liitettyinä verkkoon, jolloin niin sanottujen rosvotukiasemien asentaminen ei ole mahdollista. Yrityspuolen langattomaan verkkoon tullaan asentamaan WPA2-PSK TKIP/AES-vaihtoehto riippuen laitteistojen yhteensopivuudesta. Hieman iäkkäämmät laitteet eivät välttämättä tue AES-salausta, jolloin valitaan WPA-TKIP.

5 POHDINTAA

Langaton verkkotekniikka on vuosien saatossa kehittynyt merkittäväksi osaksi verkkostandardeja. Mobiliteetti ja laitteiden liikuteltavuus on yhä vain tärkeämmässä osassa verkostoitumista sen helppouden ja käytännöllisyyden takia. Vaikka langattomassa viestinnässä on myös heikkouksia, ovat tekniikasta saadut hyödyt silti haittoja huomattavasti suuremmat. WLAN-verkon helppo asennus, hallittavuus, käyttöönotto sekä kohtuullisen helppo suojaaminen ovat avaintekijöitä WLAN-tekniikoiden suurelle menestykselle. Tämä ei kuitenkaan tarkoita sitä, että WLAN olisi aina paras mahdollinen ratkaisu kodin tai yrityksen verkkorakenteelle. Mielestäni paras mahdollinen tulos saadaan yhdistelemällä verkkotekniikoita. Yhteisten standardien avulla saadaan aikaiseksi hyvin kommunikoiva ja toimiva kokonaisuus, mikä on myös hyvin vikasietokykyinen. Lähtökohtaisesti verkkoon ei ole hyödyllistä lisätä laitteita, joita ei tarvita.

Langattoman lähiverkon tulevaisuus näyttää erittäin lupaavalta, sillä tekniikan kehittyessä päästään yhä vain häiriösietokykyisempiin langattomiin yhteyksiin. Ehkäpä tulevaisuudessa kaikki tiedonsiirto tapahtuu radiotaajuuksien avulla, jolloin kytkinten, reitittimien, palvelimien ja tukiasemien asentaminen olisi uskomattoman helppoa. Suuria kaapeliratkaisuja ei enää tarvitsisi ottaa huomioon rakennuksen suunnittelu- ja rakennusvaiheessa, vaan lähes mihin tahansa rakennukseen voidaan asentaa verkko helposti ja edullisesti. En kuitenkaan usko, että tämä tulee tapahtumaan lähivuosina vaan puhutaan lähinnä vuosikymmenistä. WLAN-tekniikka on kuitenkin suhteellisen nuori keksintö ja kehittämismahdollisuudet ovat rajattomat.

Matkapuhelimet ovat laajentamassa käyttöaluettaan vuosi vuodelta, ja tämä vaikuttaa myös verkkotekniikoiden kehitykseen. Lähestulkoon kaikki nykyiset älypuhelimet tukevat jotakin WLAN-standardia. Langattoman verkon käyttöalue on myös hyvin merkittävässä osassa kannettavien tietokoneiden verkkoyhteyksiä, sillä jokaisessa uudessa kannettavassa tietokoneessa on jonkin luokan sisäänrakennettu langaton verkkokortti. Useat koulut panostavat myös enemmän kannettavien tietokoneiden hankintaan, jolloin WLAN-yhteydet tulevat olemaan merkittävässä osassa luokkien verkkoyhteyksiä.

Teoriapohjan avulla pystyin toteuttamaan selkeän ja hyvin toimivan langattoman verkkosuunnitelman Santapark Oy:lle. Lähdekirjallisuudesta saatu tieto oli korvaamatonta lopullisen lähiverkkoyhteyden suunnitelman toteuttamisessa. Santaparkin verkkosuunnitelma tullaan mahdollisesti toteuttamaan heti sesonkiajan päätyttyä, kun yritystiloissa olevien asiakkaiden määrä vähenee.

Opinnäytetyön teko ei ollut täysin ongelmatonta, sillä käytössä olevien laitteiden valmistaja- ja ikäerot, lähdekirjallisuuden iäkkyys sekä työn toteuttamisen viivästymiset toivat oman lisän jo suhteellisen haastavaan aiheeseen. Laitevalmistajien tekniset eroavaisuudet pystyttiin väistämään kohtuullisen pienin teoin eikä lähdekirjallisuuden iäkkyys vaikuttanut tiedon paikkansa pitävyyteen. Työn viivästyminen vaikutti lähinnä vain omaan valmistumiseeni, mutta itselleni tärkeämpänä asiana pidän pätevää ja merkityksellistä opinnäytetyötä.

Ennen opinnäytetyön aloittamista minulla oli hyvin skeptinen mielikuva langattomista lähiverkoista ja sen käyttämästä tiedonsiirtotavasta, mutta ehkäpä tästä syystä aihe kiinnosti minua hyvin paljon. Halusin saada selville, onko mahdollista toteuttaa yrityskäyttöön toimiva langaton verkkototeutus. Yllätykseksenі joudun toteamaan, että tekniikka on hyvin varteenotettava niin kotikuin yrityskäytössä. Olen siirtynyt itsekin lähestulkoon langattomaan aikakauteen ja kotini verkkoa kattaa myös langaton verkkoyhteys, jota käyttää kaksi kannettavaa tietokonetta sekä älypuhelin. Ongelmia verkon suhteen ei ole ilmennyt, vaikka rakennuksessa on yli kymmenen muiden asukkaiden WLAN-verkkolaitteita.

Lopuksi voisin antaa vihjeen langatonta verkkoa kotiinsa tai yritykseensä suunnitteleville. Pyri asentamaan jokainen paikallaan oleva laite verkkokaapelilla aina jos vain on mahdollista, sillä tämä vähentää huomattavasti verkon ruuhkaisuutta ja lisää sen tehokkuutta. Langatonta yhteyttä on parasta käyttää vain laitteissa, joita tullaan siirtämään huoneesta tai paikasta toiseen. Verkko on suositeltavaa aina suojata jollain salaustekniikalla.

LÄHTEET

Geier, J. 2005. Langattomat verkot - perusteet. PL 700: Edita Publishing Oy.

Granlund, K. 2001. Langaton tiedonsiirto. 1. painos. Jyväskylä: Docendo Finland Oy.

Granlund, K. 2007. Tietoliikenne. 1. painos. Jyväskylä: WSOYpro/Docendo Finland Oy.

Hakala, M. – Vainio, M. 2005. Tietoverkon rakentaminen. 1. painos. Jyväskylä: Docendo Finland Oy.

Home WLAN 2011. WLAN Roaming. Osoitteessa http://www.home-wlan.com/WLAN-roaming.html. 20.11.2011.

Jaakohuhta, H. 2005. Lähiverkot - Ethernet. 4. uudistettu painos. PL 700: Edita Publishing Oy.

Juuti, P. 2009. Bitit, bytet, tavut ja pikselit sekoittavat Internetin käyttäjiä. Osoitteessa http://yle.fi/alueet/keski-suomi/2009/08/tausta_ bitit_bytet_tavut_ja_pikselit_sekoittavat_internetin_ kayttajia_959950.html. 19.11.2011.

McKeag, L. 2004. WLAN Roaming - the basics. Osoitteessa http://features.techworld.com/mobile-wireless/435/ wlan-roaming--the-basics/. 15.10.2011.

Media Road 2011 Osoitteessa http://www.mediaroad.com/products/ speedcheck/free_tools/unit_convert/. 5.12.2011.

Microsoft 2012. How 802.11 Wireless Works. Osoitteessa http://technet.microsoft.com/en-us/library/cc757419 (v=ws.10).aspx. 3.1.2012.

Mitchell, B. 2011. How is Network Performance Measured? Osoitteessa http://compnetworking.about.com/od/basicnetworkingfaqs/f/ bandwidthunits.htm. 2.11.2011

Odom, W. 2005. Tietoverkot - perusteet. PL 700: Edita Publishing Oy.

Puska, M. 2005. Langattomat lähiverkot. Talentum Media Oy ja Matti Puska.

Rackley, S. 2007. Wireless Networking Technology. Great Britain.

Seleborg, S. 2007. About AES - Advanced Encryption Standard. Osoitteessa www.axantum.com/axcrypt/etc/About-AES.pdf. 7.10.2011.